PROPUESTA DE ADAPTACIÓN DEL FRAMEWORK DE CIBER SEGURIDAD DE NIST A LOS SECTORES QUE SOPORTAN INFRAESTRUCTURAS CRITICAS EN COLOMBIA
ENFOQUE SOBRE EL SECTOR DE LAS TELECOMUNICACIONES

JAVIER SANTORO ARRIETA

RICARDO RODRÍGUEZ GUZMÁN

UNIVERSIDAD PILOTO DE COLOMBIA

FACULTAD DE INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ, D.C.

2016

PROPUESTA DE ADAPTACIÓN DEL FRAMEWORK DE CIBER SEGURIDAD DE NIST A LOS SECTORES QUE SOPORTAN INFRAESTRUCTURAS CRITICAS EN COLOMBIA
ENFOQUE SOBRE EL SECTOR DE LAS TELECOMUNICACIONES

JAVIER SANTORO ARRIETA

RICARDO RODRÍGUEZ GUZMÁN

Trabajo de grado para optar al título de
Especialista en Seguridad Informática

Asesor:
Ing. Álvaro Escobar

UNIVERSIDAD PILOTO DE COLOMBIA

FACULTAD DE INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ, D.C.

2016

Nota de aceptación

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, D.C., Mayo 17 de 2016.

Dedicado a nuestros padres y todas aquellas personas que de una forma u otra ayudaron a que éste trabajo se pudiera llevar a cabo satisfactoriamente. A todas esas personas que nos aconsejaron, nos enseñaron, nos apoyaron y no nos dejaron desfallecer. Esas personas que nos ayudan cada día a ser mejores de lo que hemos sido hasta ahora.

CONTENIDO

pág.

LISTA DE GRÁFICAS

pág.

LISTA DE CUADROS

Pág.

GLOSARIO

AMENAZA (THREAT): la posibilidad de compromiso, pérdida o robo de información o de servicios y recursos que la soportan. Una amenaza puede ser definida por su origen, motivación o resultado y puede ser deliberada o accidental, violenta o subrepticia, externa o interna.

ATAQUES DIRIGIDOS: ataques muy dañinos en los que los atacantes no actúan de forma indiscriminada, sino que utilizan código malicioso diseñado para infectar a usuarios, empresas u organizaciones concretas.

ATAQUE DDOS: ataque de negación de servicio DoS, Ataque distribuido de denegación de servicio. Es un ataque a un ordenador o red que provoca una saturación en el ancho de banda o una sobrecarga en los recursos hasta que los servicios del ordenador o la red dejan de estar disponibles para los clientes. Se pretende dejar sin servicio a determinados usuarios enviando mensajes de forma masiva a un servidor desde un gran número de sistemas infectados. La negación de servicio también puede producirse cuando un código malicioso desconecta los recursos.

ATAQUE MAN-IN-THE-MIDDLE: ataque en el que se utilizan tácticas de observación e interceptación para leer, insertar y modificar mensajes intercambiados entre dos usuarios o sistemas.

BRECHA DE SEGURIDAD: en términos de Ciberseguridad informática se define como una deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal. La seguridad informática permite asegurarse que los recursos del sistema se utilizan de la manera en la que se espera y que quienes puedan acceder a la información que en él se encuentran sean las personas acreditadas para hacerlo.

CIBERATAQUE: ataque contra la infraestructura informática de un país. Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

CERT: Computer Emergency Response Team (Equipo de respuestas a emergencias informáticos).

CSIRT: Computer Security Incident Response Team (Equipo de respuestas a incidentes informáticos).

CIBEREVENTO: cualquier suceso observable en un sistema de información y comunicaciones.

CIBERINCIDENTE: Ciberevento adv en un sistema de información y comunicaciones o la amenaza de que se produzca.

CIBERSEGURIDAD: es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberespacio. La Ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberespacio.

CIBERDEFENSA: la aplicación de medidas de seguridad para proteger los diferentes componentes de los sistemas de información y comunicaciones de un Ciberataque.

CIBERESPACIO: el mundo digital generado por ordenadores y redes de ordenadores, en el cual personas y ordenadores coexisten y el cual incluye todos los aspectos de la actividad "*online"*.

CIBERTERRORISMO: un Ciberataque para causar la inutilización o interrupción de redes de ordenadores o comunicaciones para generar temor o intimidar a la sociedad con un objetivo ideológico.

COBIT: control Objectives for Information and related Technology.

GESTIÓN DE RIESGOS: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

GESTIÓN DEL RIESGO: aproximación sistemática, basada en la valoración de las amenazas y las vulnerabilidades, para la determinación de las contra-medidas necesarias para la protección de la información o los servicios y recursos que la soportan.

INFRAESTRUCTURAS CRÍTICAS: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción o destrucción tendría un grave impacto sobre los servicios públicos esenciales.

ISO: International Organization for Standarization.

NIST: National Institute of Standards and Technology.

PHISHING: los ataques de "Phishing" usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros aunque no en la mayoría de ellos). Para alcanzar al mayor número posible de víctimas e incrementar sus posibilidades de éxito, utilizan el correo basura ("spam") para difundirse.

RIESGO: la probabilidad de que una vulnerabilidad sea explotada con éxito por una amenaza produciendo un compromiso de confidencialidad, integridad y/o disponibilidad y daños.

VULNERABILIDAD: una debilidad que puede ser aprovechada por una amenaza.[1]

[1] CNI.ES. CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO. [En línea]. Disponible en: https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf [Consultado 16 Enero 2016].

INTRODUCCIÓN

En la actualidad, la necesidad de crear y adoptar un ámbito, y una infraestructura de seguridad fuerte dentro de una entidad, sector u organización es cada día más evidente. Las infraestructuras críticas de un país son complejas, basadas en sus sistemas físicos y cibernéticos, forman la línea de vida de una sociedad moderna, y su fiable y segura operación es de vital importancia para la seguridad nacional y la vitalidad económica.

La necesidad de protegerse ante posibles ataques de diferentes índoles físicas o cibernéticas, permite que las organizaciones o sectores de vital importancia para el desarrollo de un país se enfoquen cada día más en verificar si los esquemas de defensa implementados actualmente se encuentran funcionando de forma idónea y cumplen con sus objetivos de seguridad; en más de un sentido, los sistemas cibernéticos forman parte de la columna vertebral de la infraestructura critica de una nación, lo cual significa que un incidente de escala mayor de seguridad en cualquier tipo vital de sistema cibernético, podría tener un impacto significativo sobre las operaciones fiables y seguras de los sistemas físicos que dependen de ella.

Las organizaciones de vital importancia para Colombia, como lo son las que pertenecen al sector de telecomunicaciones, se encuentran expuestas cada día a nuevos tipos de riesgos y ataques de tipo cibernético (conocidos también como “Ciberataques”), que buscan entre sus objetivos afectar la funcionalidad de un sector crítico. Reportes y documentos expedidos recientemente por parte del gobierno Colombiano, demuestran la creciente amenaza de ataques cibernéticos en número y complejidad enfocados al sector de las telecomunicaciones y a otros tantos sistemas con infraestructuras críticas para el país.

Es así como nace la necesidad de adoptar un modelo de referencia, un Framework desarrollado por organizaciones e institutos líderes en el campo de la

Ciberseguridad, y basado en un proceso reiterativo diseñado para evolucionar en sintonía con los cambios en las amenazas, procesos y tecnologías. Como uno de los enfoques de esta investigación, se busca que este modelo pueda ser visto como una iniciativa en materia de Ciberseguridad en Colombia en cuanto a defensa y mejora de los modelos de gestión de la seguridad ya implementados en las organizaciones y sectores vitales que cuentan con infraestructuras críticas. ¿Pero qué se entiende por infraestructura crítica? El mismo concepto puede tomarse del entendimiento de los sistemas sobre los cuales se maneja un país y su forma de vida actual, el cual debe asegurar como mínimo, la prestación de aquellos servicios considerados como esenciales (Agua, Alimentación, Energía, Industria Química, y Nuclear, Transporte, Telecomunicaciones, Sistema Financiero, entre otros). Por tanto, al tener una mejor concepción de la necesidad de proteger las infraestructuras críticas de un país o región, se puede entender cómo surge o nace la necesidad de que exista un posible modelo que ponga en práctica nuevas estrategias, controles y políticas, que garanticen dichos servicios ante vigentes y futuras amenazas derivadas de posibles ataques de origen (para el presente caso de estudio) cibernético.

El Framework de Ciberseguridad de NIST comprende las prácticas líderes de diversos organismos que han demostrado ser exitosas cuando se implementan y cuya adopción puede resultar ventajosa para las empresas a través de prácticamente todas las industrias.

1. FORMULACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Definición del problema. Hoy día las telecomunicaciones son un componente vital en la infraestructura nacional y juegan un papel importante en la seguridad nacional, así como de su desarrollo económico y financiero. El sector de las telecomunicaciones provee un universo muy complejo y dinámico que consiste en un conjunto global de las partes interesadas.

Los operadores de telecomunicaciones desempeñan un papel importante, ya que proveen directamente servicios de comunicaciones dirigidos a consumidores, industria y gobierno. Estos servicios y las telecomunicaciones, son factores significativos para poder mantener un modelo económico de vida moderna; algunas industrias y organizaciones por ejemplo, son incapaces de alcanzar sus más importantes objetivos de negocio sin la ayuda de los más actuales servicios de telecomunicaciones.

Es así como, a medida que las herramientas de telecomunicaciones se vuelven más asequibles en todo el mundo, los Ciberataques se hacen cada vez más comunes. Ataques muy publicitados con fines económicos o políticos a los proveedores de servicios de telecomunicaciones, sirven como un recordatorio a la constante necesidad de la vigilancia dentro del marco nacional de Ciberseguridad y de adaptar modelos importantes al estándar Colombiano.

Los servicios de telecomunicaciones deben poder ser establecidos de forma robusta para gestionar y asegurar una sólida defensa nacional, la respuesta a desastres, y otros servicios de emergencia. Un único Ciberataque contra un sector en particular como objetivo, podría afectar miles de servicios de los consumidores si se realiza de forma adecuada.

Los esfuerzos de las compañías para implementar medidas efectivas seguirán siendo un componente vital de una postura de seguridad nacional. La seguridad nacional requiere redes de telecomunicaciones resistentes, es decir, que puedan soportar daños y seguir prestando servicio en el caso de ataques directos de tipo físico o cibernético.

Una interrupción en un proceso vital puede llegar a ser catastrófico, la obligación de cumplir con la seguridad y el cumplimiento de la calidad en las operaciones es una cuestión difícil a pesar de que se trata de una cuestión de alta relevancia.

Debe entenderse claro está, que al momento de determinar un marco base que servirá como referencia para mejorar los aspectos de Ciberseguridad, se encontraran cierto número de diferencias entre un modelo Norte Americano y uno nacional. Sin embargo y a pesar de la complejidad de la tarea, una adaptación exitosa puede llegar a ser la referencia base para los sectores vitales en cuanto al desarrollo de una estrategia de seguridad nacional colombiana.

1.2 JUSTIFICACIÓN

Debido al nivel de madurez que existe actualmente por parte de las entidades colombianas del sector de las telecomunicaciones en cuanto al tema de Ciberseguridad, y la falta de implementación de estándares internacionales que ayuden a la mitigación de riesgos de Ciberseguridad, nace la necesidad de proponer una posible adaptación de un Framework que sea exitoso a nivel mundial; para este trabajo de investigación, se optó por adaptar el desarrollado por el Instituto Nacional de Estándares y Tecnología (Framework for Improving Critical Infrastructure Cybersecurity) al marco colombiano.

El éxito del Framework se basa en reducir el riesgo de Ciberseguridad en infraestructuras criticas utilizando como referencia normas internacionales existentes, las mejores prácticas y procedimientos que han demostrado su eficacia reflejando el buen trabajo de cientos de empresas, múltiples agencias federales, y colaboradores de todo el mundo. La aplicación de este tipo de casos de éxito en Colombia, basados en la posible adaptación del Framework, puede ofrecer ventajas regulatorias y legales que se extienden mucho más allá de la mejora de la Ciberseguridad para las organizaciones del sector de las telecomunicaciones que la adoptan tempranamente.

1.3 OBJETIVOS

1.3.1 Objetivo general

Desarrollar una propuesta investigativa para la posible adaptación del Framework de Ciberseguridad de NIST en los sectores que soportan infraestructuras críticas, con un enfoque a las empresas del sector de telecomunicaciones en Colombia.

1.3.2 Objetivos específicos

- Ayudar a que las empresas u organizaciones del sector de telecomunicaciones puedan identificar con éxito su postura actual en materia de Ciberseguridad y el estado objetivo deseado de la misma. Así mismo, identificar y priorizar las oportunidades de mejora en el contexto de un proceso continuo y repetible.

- Desarrollar una guía que de forma específica y acertada, promueva a que las organizaciones pertenecientes al sector de las telecomunicaciones en Colombia visualicen una posible implementación en un futuro, del Framework de Ciberseguridad de NIST dentro de las mismas.

2. MARCO TEÓRICO

Los sectores de vital importancia para el desarrollo de un país siempre estarán propensos a sufrir diferentes tipos de amenazas causadas por diversas fuentes y buscando diferentes tipos de objetivos. Interrupciones, daños a la información, desastres naturales, entre otros, son algunas de las posibles amenazas a las que las entidades de cualquier índole deben enfrentarse cada día. Sin embargo, y aunque el crecimiento exponencial del uso de herramientas cibernéticas dentro de las organizaciones es una realidad, así mismo no lo es la prevención ante ataques y amenazas cibernéticas a las que estas pueden estar expuestas. Aunque es conocido que sectores significativos y que soportan infraestructuras críticas, como lo es el de las telecomunicaciones se encuentra rodeado de tecnología de punta en cuanto a materia de redes y servicios, su mismo contexto no lo hace exento de una vulnerabilidad palpable y al mismo tiempo casi imperceptible en el núcleo de su negocio. Actualmente, este tipo de amenazas puede llegar a afectar el desempeño de sectores tan importantes como lo es el de las telecomunicaciones, debido a su poca implementación o en algunos casos desconocimiento en materia de Ciberseguridad.

¿Qué se entiende entonces por Ciberseguridad? La Ciberseguridad es seguridad de la información aplicada a las máquinas, computadores y las redes informáticas. Dicho tipo de seguridad abarca todos los procesos y mecanismos por los que el equipo basado en computadoras, la información y los servicios están protegidos contra el acceso no deseado o no autorizado, modificación o destrucción de la misma.

Como se mencionó anteriormente, además de estar propensas a ataques físicos o a un desastre natural, las redes de telecomunicaciones y de infraestructura crítica están expuestas a los Ciberataques. Dichos ataques, deben generar una alerta relevante en las empresas u organizaciones que cuentan con dichas infraestructuras críticas, ya que son estas mismas, quienes deben velar por mantener los servicios necesarios para conservar y asegurar la vida económica y social de un sector, una región, o bien sea, una sociedad como en las que se basan las economías modernas.

Los Ciberataques pueden ser provocados o accidentales; puede implicar ataques de otros estados-nación, grupos organizados o individuos; y puede estar motivada

por la ganancia monetaria, la mala voluntad, o intereses políticos. Los Ciberataques pueden estar dirigidos a los gobiernos, empresas o individuos. Pueden implicar el robo o destrucción de la información; el robo de servicios o activos financieros; o la destrucción de la infraestructura de hardware o software en cualquier entidad o sector. Los Ciberataques pueden resultar en pérdidas financieras, de negocios o de la interrupción del servicio, o la destrucción de la infraestructura.

Dichos ataques pueden estar dirigidos directamente a interrumpir los servicios o la infraestructura de un sector en particular, como en nuestro caso de estudio lo es el de las telecomunicaciones, tener la intención de interrumpir otro servicio, o algún dependiente del funcionamiento de los servicios de comunicación de la industria.

Los Ciberataques pueden ser lanzados en conjunto con los ataques físicos con el fin de ampliar los efectos o prevenir una respuesta eficaz. De ahí, que la conciencia en cuanto a identificar amenazas en materia de posibles Ciberataques y el conocimiento de un sólido conocimiento en Ciberseguridad sea tan significativo e importante; enfocarse en entender estas amenazas y ayudar a desarrollar políticas para prever, mitigar y responder ante diversos ataques, son de los principales objetivos de la Ciberseguridad.

El Instituto Nacional de estándares y Tecnología (NIST), está realizando constantemente llamados de acción para aquellas compañías que manejan infraestructuras críticas en países como los Estados Unidos (país fundador de dicho instituto). Fundado en 1901, el NIST es una agencia federal no reguladora dentro del Departamento de Comercio de EE.UU.

La misión de NIST es promover la innovación y la competitividad industrial Norte americana avanzando en ciencia de la medición, los estándares y la tecnología en formas que mejoren la seguridad económica y mejoren la calidad de vida de las sociedades. Es así como NIST, hace un llamado a una amplia gama de compañías que van desde las Finanzas y Cuidados de salud, hasta Energéticas y de Tecnologías de la Información, a estar preparadas para adoptar y probar que sus prácticas de Ciberseguridad son consistentes con las prácticas subrayadas en la actualidad.

Como visión general, NIST busca ser el líder mundial en la creación de soluciones de medición críticas y promover normas equitativas aplicables a organizaciones y

entidades. Los esfuerzos de NIST buscan estimular la innovación, la competitividad industrial y mejorar la calidad de vida.

El desarrollo de un Framework de Ciberseguridad por parte del NIST se centra en el uso de factores de negocio para guiar las actividades de Ciberseguridad, teniendo en cuenta los riesgos de seguridad cibernética como parte de los procesos de gestión de riesgos de una organización o sector.

Dicho Framework busca ayudar a que una organización pueda alinear sus actividades de seguridad cibernética con los requerimientos del negocio, la tolerancia al riesgo y los recursos disponibles. Es importante resaltar, que uno de los objetivos primarios de NIST con la creación del Framework de Ciberseguridad, es complementar y más no reemplazar, el proceso de gestión de riesgos actual de una organización y su programa de seguridad cibernética; alternativamente, una organización sin un programa de seguridad cibernética existente, puede utilizar el Framework como referencia para establecer uno.

Para Colombia, el tema de la Ciberseguridad viene desarrollándose de forma continua a través de los últimos años intentando alcanzar un estado óptimo en cuanto a defensa en el campo de amenazas cibernéticas y delincuencia digital. La adopción de tecnología por parte de las organizaciones y los sectores de vital importancia para el país es cada vez mayor, y el uso de la misma viene de la mano con las amenazas y vulnerabilidades que representan. Es debido a esto, que los retos para proteger a los ciudadanos, a los sectores más significativos y al propio Estado elevan la importancia del tema.

Siguiendo esta línea de ideas, es por esto que Colombia debe acelerar su proceso en materia de política de Seguridad y Defensa Cibernética. Si se tiene en cuenta el acelerado ritmo de adopción de las TIC en el país, sería lógico pensar que una de las áreas de enfoque principal en materia de Ciberseguridad se trataría del sector de las telecomunicaciones como uno de los de importancia relevante; tan solo en el trascurso de los años 2010 a 2014 el ritmo con el que ha crecido la demanda y el uso de medios electrónicos, conexiones a internet y comercio electrónico, se ve reflejada de una forma exponencial.

Partiendo del hecho que el uso de las TIC debe ser fiable y seguro para los usuarios que las manejan y manipulan, actualmente la CRT (Comisión de Regulación de telecomunicaciones) ha implementado un estudio, propuesto en el año 2007, para la estrategia nacional en tema de Ciberseguridad, proponiendo y

desarrollando diferentes tipos de acciones y estrategias. El “Estudio para la implementación de una Estrategia Nacional de Ciberseguridad” desarrollado por la CRT, describe los principales requisitos de seguridad para redes de telecomunicaciones. Dentro de lo que el estudio busca implementar podemos encontrar la protección de la confidencialidad de los datos y los intereses de los consumidores, asegurar la fiabilidad de las transacciones electrónicas y el comercio en línea, e instaurar el control de los mismas, mejorar la calidad de las redes mundiales y regionales, así como mantener la interconexión y el inter funcionamiento de las mismas, entre otras que buscan abarcar la realidad en cuanto a amenazas cibernéticas.

En cuanto al sector de las telecomunicaciones, la CRT busca con este estudio plasmar y desarrollar documentos, procesos que describirán los principales requisitos de seguridad para las redes de telecomunicaciones, la arquitectura de seguridad para los sistemas de comunicaciones de extremo a extremo, y las diferentes acciones nacionales e internacionales que se han venido realizando en el ámbito de la seguridad de las redes de información y comunicación. De forma genérica, la CRT busca marcar un lineamiento en forma de recomendación sin abordar requisitos sobre redes específicas.

Así mismo, y en forma de recomendación u orientación de naturaleza genérica, la CRT busca que en el ámbito de seguridad en cuanto a redes de información y comunicación en el sector de las telecomunicaciones en Colombia, se cumplan ciertos tipos de “Requisitos de seguridad para las redes de Telecomunicaciones”. De esta forma, se busca poder identificar las amenazas a la seguridad de las redes de telecomunicaciones en general, así como orientar a la planificación de las contramedidas que se pueden prever para disminuir los riesgos que surgen de las amenazas en el campo cibernético.

Las propuestas implementadas por la CRT en el tema de seguridad bajo el lineamiento de recomendaciones en el sector de redes y telecomunicaciones, puede ser usada para dirigir el desarrollo de definiciones completas de política de seguridad, reacción a incidentes y las arquitecturas de tecnología, tomando en cuenta los objetivos de negocio durante la etapa de definición y planificación específica de cada entidad. La CRT busca de igual forma que la propuesta de implementación al modelo Colombiano, también se pueda usar como el fundamento de una evaluación del programa de seguridad, que examinaría la forma en que las entidades enfrentan los diversos posibles riesgos o amenazas mientras se introducen nuevas políticas y procedimientos, y la nueva tecnología que se implementa.

Como conclusión de las medidas de seguridad tomadas sobre el modelo colombiano en el sector de las redes de telecomunicaciones, se busca que en la actualidad, estas medidas deban estar encaminadas hacia objetivos logrados y no hacia la forma en cómo estos se están logrando.

En cuanto a la normatividad Colombiana, las medidas de acción nacional impuestas por el país, incluye diferentes tipos de medidas y leyes que buscan establecer los parámetros y lineamientos en materia de seguridad informática y telecomunicaciones. Algunos ejemplos son, la Ley 527 de 1999 que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, la Ley 962 de 2005, la cual dicta disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. El Decreto 1747 de 2000 , introdujo nuevas funciones para las entidades de certificación relacionadas con la obligación de abstenerse de acceder o almacenar la clave privada de un usuario, la obligación de mantener el control de su clave privada, y establecer las medidas necesarias para que no sea conocida por el público, garantizar la confidencialidad de la información que no figure en el certificado, capacitar y advertir a los usuarios sobre las medidas de seguridad que deben observar para la utilización de la firma y los certificados digitales, ente otros.

En el año 2008, la CRT publicó el documento “Recomendaciones al Gobierno Nacional para la implementación de una Estrategia Nacional de Ciberseguridad”, dentro del contexto de acciones adelantadas. Dentro del documento publicado se realizaron diferentes tipos de recomendaciones enfocadas al sector de las telecomunicaciones y a la disuasión del crimen cibernético e incluye propuestas a la vigilancia, análisis y respuesta a estos incidentes. Así mismo, se desarrollaron acciones de estrategia dentro del mismo documento como los son la necesidad de la acción nacional para hacer frente a las amenazas y las vulnerabilidades de la infraestructura nacional, establecer un mecanismo nacional de respuesta a incidentes denominado (N-CSIRT) y establecer mecanismos de cooperación entre el gobierno y las entidades del sector privado a nivel nacional.

En el contexto del estado actual del sector de telecomunicaciones en Colombia en materia de Ciberseguridad y de seguridad informática, y basados en los estudios, documentos y publicaciones del CRT, se pueden hallar diferentes tipos de evidencias. Actualmente según los estudios mencionados con anterioridad, la inversión de los operadores en seguridad de la información está enfocada a la protección de la red y a la protección de los datos críticos, pero dejan a un lado la

contratación de personal calificado y la realización de pruebas y evaluaciones de seguridad con regularidad; mucho de lo anterior mencionado recae en la falta de interés o desconocimiento acerca del tema por parte de los miembros directivos de los sectores relacionados.

Para el año 2009, se adelantó el desarrollo de una iniciativa que buscaba conocer la tendencia mundial en normas de seguridad en redes de telecomunicaciones, marcos de arquitecturas de seguridad y seguridad de gestión de redes, con el propósito de elaborar recomendaciones para el ámbito nacional. Dentro de otros aspectos, la agenda del 2009 pretende conocer además de estudiar las principales herramientas de seguridad en Internet e identificar las diferentes soluciones que proveedores de seguridad están implantando en Colombia.

3. METODOLOGÍA

Para la realización del presente trabajo de grado se ha tomado un enfoque investigativo con el propósito de profundizar en el área de la Ciberseguridad. Para ello, y tomando como referencia al Framework de Ciberseguridad desarrollado por NIST, se desarrollaron una serie de pasos que de forma estructurada, buscan mostrarnos el estado actual de los esquemas de Ciberseguridad en Colombia y como llevarlos hasta un modelo que actualmente es aceptado internacionalmente, implementado y aplicado con éxito.

Dichos pasos, descritos en este documento de investigación, abarcan:

- Estado del arte a nivel mundial y en Colombia en cuanto a Ciberseguridad.

- Análisis del reporte en cuanto al estado actual y postura de Ciberseguridad e infraestructuras críticas de los países que pertenecen a la OEA (Organización de los Estados Americanos).

- Desarrollo de un caso de estudio el cual habla acerca de las infraestructuras críticas en Colombia y del sector de las redes de Telecomunicaciones.

- Recorrido por el framework de Ciberseguridad de NIST, sus etapas, su estructura y los elementos que lo componen.

- Desarrollo de una guía de ayuda para entender el Framework de Ciberseguridad, el uso del mismo y su posible implementación en sectores que soporten infraestructuras críticas.

- Identificación de brechas existentes entre el modelo propuesto por NIST y lo encontrado en el modelo colombiano.

- Recomendaciones realizadas a partir de las brechas identificadas para una posible adaptación del Framework de Ciberseguridad al modelo colombiano.

4. DESARROLLO DEL PROYECTO

Basándose en documentos que existen en la actualidad, por parte de organizaciones que actualmente poseen cierto peso a nivel americano como lo es la OEA y empresas del sector de la seguridad informática y Ciberseguridad, como Trend-micro y Symantec, se logró un acercamiento a resultados que exponen el estado actual de los países que hacen parte de la Organización de los Estados Americanos en cuanto a ataques cibernéticos y el manejo que se la da a la Ciberseguridad.

El documento desarrollado por la OEA, “Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas”, el cual ha servido como material de referencia para los propósitos de este trabajo de investigación, se desarrolló como un documento integral del cual los Estados Miembros de dicha organización, los operadores de las infraestructura críticas y otros, puedan sacar conclusiones útiles y entender mejor sus posturas en cuanto a Ciberseguridad, así como las principales amenazas cibernéticas que afectan a la infraestructura crítica en América.

La colaboración que realiza la OEA en la actualidad es de carácter crítico al aportar de forma significativa para las infraestructuras críticas de los países de América, los instrumentos para fomentar y alinear de forma acertada las políticas en cuanto a Ciberseguridad de todo el continente; para enfrentar las amenazas cibernéticas, la OEA busca entender las capacidades de seguridad cibernética de los países de América y las tendencias de los ataques cibernéticos como el primero paso básico hacia el fortalecimiento de la Ciberseguridad y la capacidad de respuesta de cada uno de estos países miembros de su organización.

Continuando entonces con lo expuesto en el informe de la OEA, se encontraron aspectos de carácter relevante, como lo expuesto en el 2013 donde se observó un aumento de las violaciones de datos, troyanos implantados en el sistema bancario, malware orientado a dispositivos móviles y otras amenazas de carácter importante en la red. Los constantes ataques por parte de criminales cibernéticos, siguió presentando desafíos a muchos de los países más importantes de la región andina. De igual forma, el informe expone un análisis en profundidad de las tendencias observadas y se proporcionan indicaciones acerca de ciertas medidas preventivas que pueden tomar los usuarios para protegerse de manera más eficaz. El informe detalla, además, una cantidad de nuevas tendencias y vulnerabilidades alarmantes registradas a nivel mundial, así como las específicas de América Latina y el Caribe.

4.1 RESULTADOS DEL ESTUDIO REALIZADO POR LA OEA

Debido entonces al éxito del estudio realizado en 2013 “Tendencias de la Seguridad Cibernética y las Respuestas de los Gobiernos de América Latina y el Caribe”, el cual contó con la cooperación de Symantec, la OEA y Trend Micro, para realizar una encuesta en materia de ataques informáticos y Ciberseguridad, cuyos resultados buscan brindar otra visión del estado de la seguridad de los países miembros de la OEA. Dicha encuesta sin precedente la cual contó con la participación de más de 20 Estados Miembros de la OEA ofrece un panorama del estado actual de la seguridad cibernética alrededor de la infraestructura crítica de la región y de las tendencias de las amenazas que enfrentan estas organizaciones clave.

La información obtenida y reunida mediante dicha encuesta, ofrece una importante perspectiva de los ataques cibernéticos sufridos por las organizaciones de infraestructura crítica en la región, el apoyo que ofrecen los gobiernos locales, las medidas y políticas de seguridad cibernética de las organizaciones, así como su preparación para enfrentar dichos ataques, y dentro de las cuales no solo se encuentran el sector de las telecomunicaciones, que hace parte de este proyecto de investigación, sino también las que competen a otros sectores de vital importancia como los son los sectores de transporte, salud, banca, energía, entre otros.

Muchos de los hallazgos de la encuesta presentada por la OEA, se pueden llegar a relacionar directamente, con algunas de las problemáticas propuestas para esta

investigación, y que muestran la actualidad acerca de los ataques de carácter cibernético, que de forma evolutiva podrían llegar a atentar contra las organizaciones que de una forma u otra soportan infraestructuras críticas.

La OEA propone que junto con los resultados obtenidos a través de estos tipos de encuestas y estudios, los nuevos conocimientos ayudarán a guiar todo tipo de investigaciones en el futuro para proteger a dichas organizaciones contra posibles amenazas y ataques cibernéticos.

El informe “Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas”, también brinda un panorama integral de la seguridad cibernética en América, con el aporte de 30 de los 32 países de América Latina y el Caribe. Los participantes en la encuesta pertenecen a agencias de gobierno, así como a industrias críticas como las comunicaciones, banca y finanzas, manufactura, energía y seguridad, entre otras; dentro de lo mencionado por la OEA y Symantec en sus informes se destaca el hecho de que los atacantes están cada vez más interesados en robar datos para provocar caos y confusión mediante los ataques dirigidos a los sistemas de control (SCADA).

Dentro de los hallazgos observados en los resultados del informe y de la encuesta, encontramos a nivel general que:

- Gran parte de los entrevistados dejaron claro que los ataques dirigidos a la infraestructura son un peligro claro y presente, mientras que sólo un menor porcentaje de ellos pudo decir que no habían visto este tipo de ataques.

- Cuando se les pidió hacer una descripción del panorama de amenazas, los participantes de la encuesta aseguraron que éstas están siendo muy severas, mientras que algunos calificaron como desalentador el futuro de asegurar estas infraestructuras. Para la mayoría de los encuestados, la frecuencia de los ataques está aumentando o se mantiene constante, en tanto que los ataques son cada vez más sofisticados.

- Entre los factores positivos, los entrevistados indicaron que estaban preparados o algo preparados para enfrentar un ataque cibernético. Así mismo, las organizaciones han implementado tecnologías, políticas y procedimientos que pueden ayudar a proteger su entorno.

- Este reporte también revela la falta de asociación proactiva entre los gobiernos y las organizaciones privadas de la región. Una escueta mayoría de los encuestados de la industria privada y del gobierno reportó que no hay un diálogo o sólo hay diálogos informales entre estos socios clave.

- Otro impedimento para enfrentar estas amenazas en evolución son los bajos presupuestos. La mayoría de los encuestados dijo que existen desafíos que pueden dificultar la defensa continua contra los ataques dirigidos a sus infraestructuras críticas.

- Si bien las organizaciones de América han hecho un buen trabajo para proteger la infraestructura crítica contra los ataques, se acerca un punto crítico. Debido a que la frecuencia y la sofisticación de los ataques continuarán o se agravarán y se enfocarán no sólo en afectar a la infraestructura crítica sino también en comprometer la información vital que pudiera usarse en el futuro, los defensores pronto podrían no tener el apoyo necesario para prevenirlos. La falta de financiamiento y de liderazgo gubernamental en esta área deja a los profesionales encargados de la seguridad cada vez con menos recursos para afrontar sus necesidades en cuanto a Ciberseguridad. Más que eso, los gobiernos de la región necesitan tender la mano a los encargados de la infraestructura crítica que buscan ayuda y guiarlos para ofrecer mejor protección contra los crecientes ataques a este sector crucial.

Como se puede concluir, a raíz de los hallazgos obtenidos a través de las respuestas de los encuestados por la OEA, el panorama aunque en algunos puntos pareciese ser claro para muchas organizaciones a nivel latinoamericano en cuanto a su entorno en materia de Ciberseguridad, así como los ataques, amenazas y medidas a enfrentar, no parece ser del todo seguro y en algunos puntos parece haber cierta incertidumbre. Sin embargo, puede observarse que en gran medida, las organizaciones que soportan infraestructuras críticas, en los diferentes sectores de una sociedad, son conscientes de la tendencia creciente y critica en cuanto a ataques y amenazas cibernéticas como una realidad palpable y de crecimiento exponencial.

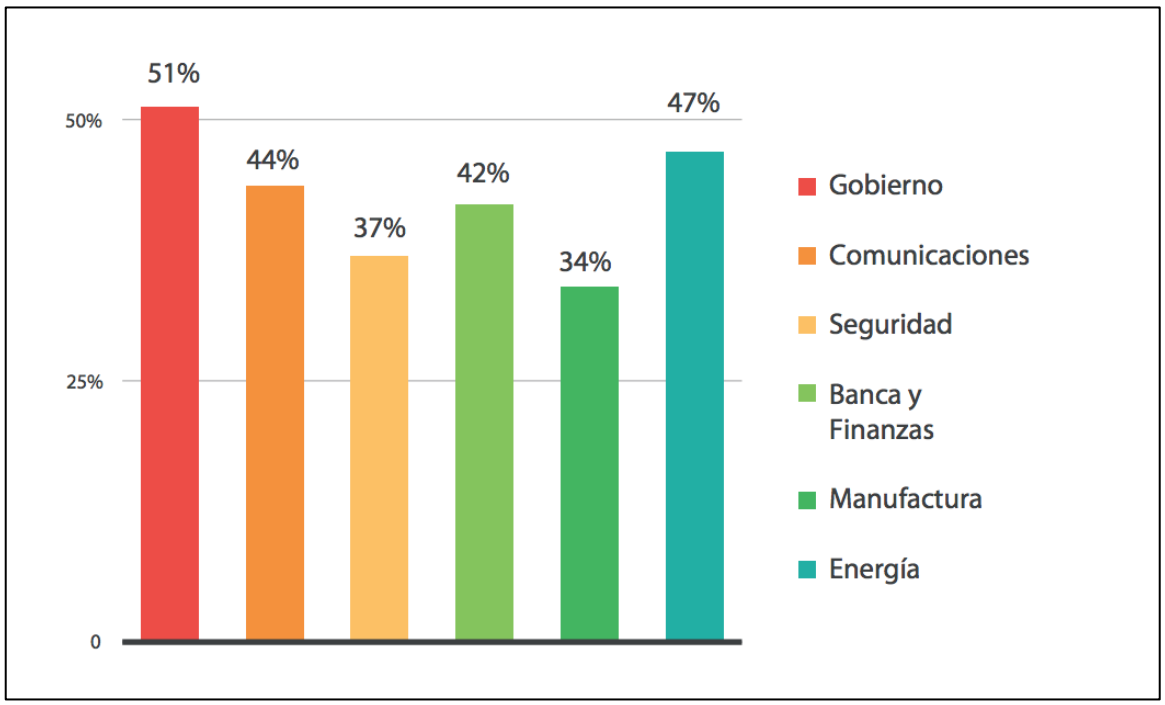
¿Se están tomando en la actualidad las medidas necesarias para enfrentar los riesgos de Ciberseguridad a nivel latino americano o en un país como Colombia? Según los hallazgos de los estudios e investigaciones realizados por la OEA, el tema parece no tener la relevancia que amerita, y en el caso de Colombia no parecer ser la excepción.

A continuación se expondrán algunos de los resultados de la encuesta los cuales tienen que ver con la investigación propuesta en este documento. La primera parte de la encuesta evalúa el estado del panorama de las amenazas en estas regiones y cómo se perpetran los ataques prevalentes y sofisticados.

Experiencia con varios incidentes

- Porcentaje de Organizaciones que experimentaron intentos de eliminar o destruir información por tipo.

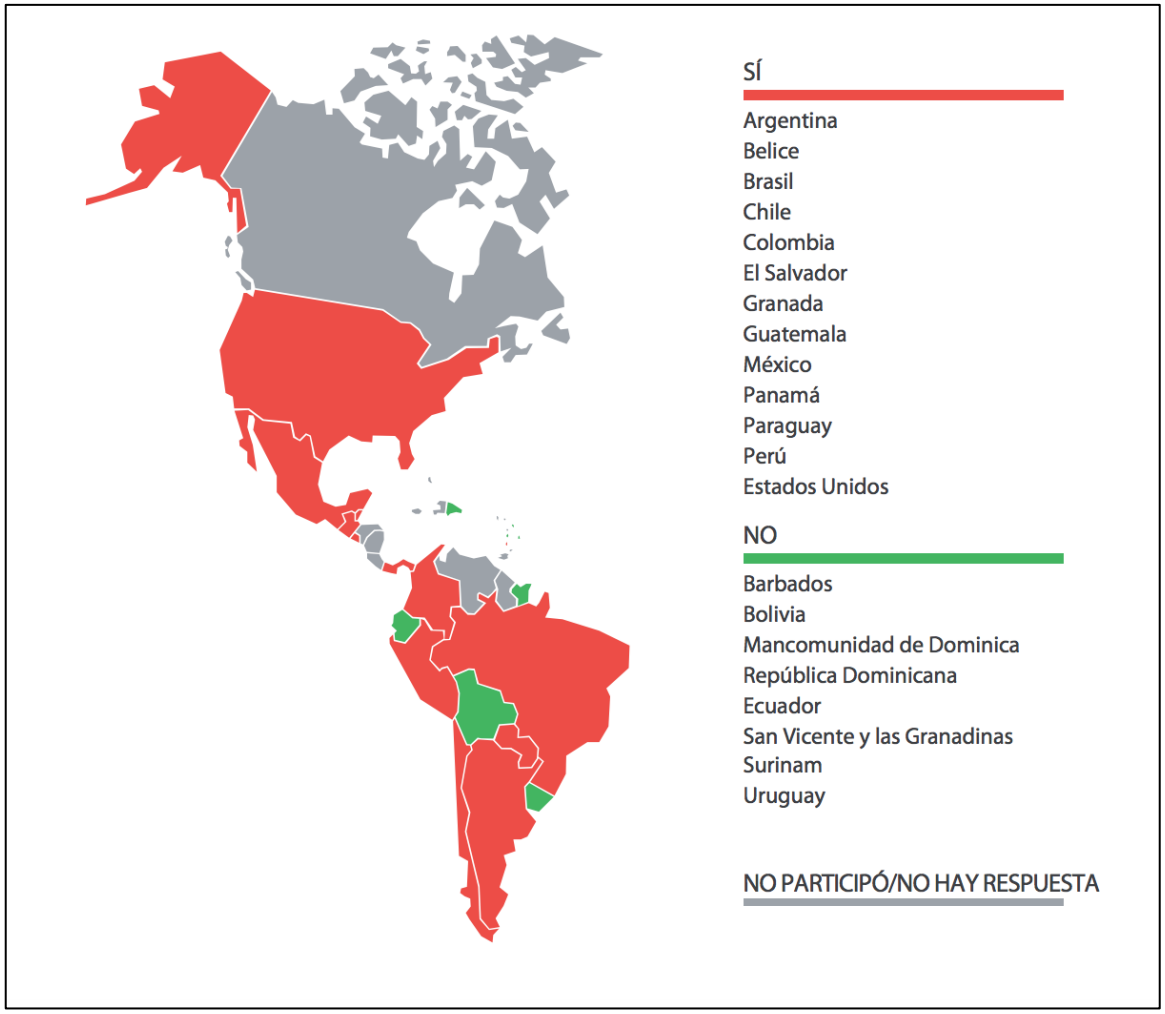
Gráfica 1. Organizaciones afectadas



Fuente: Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas [en línea]. Organization of America States, Trend Micro, 2015 [consultado 24 de Octubre de 2015]. Disponible en Internet: https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

- De acuerdo con los resultados de la encuesta, los sectores de gobierno y energía son las dos principales industrias que sufren ataques destructivos por amenazas, seguidos por los de comunicaciones y de banca y finanzas.
- Las Instituciones Gubernamentales que experimentaron intentos de manipulación de su equipo a través de una red/sistema de control por País.

Gráfica 2. Países afectados



Fuente: Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas [en línea]. Organization of America States, Trend Micro, 2015 [consultado 24 de Octubre de 2015]. Disponible en Internet: https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

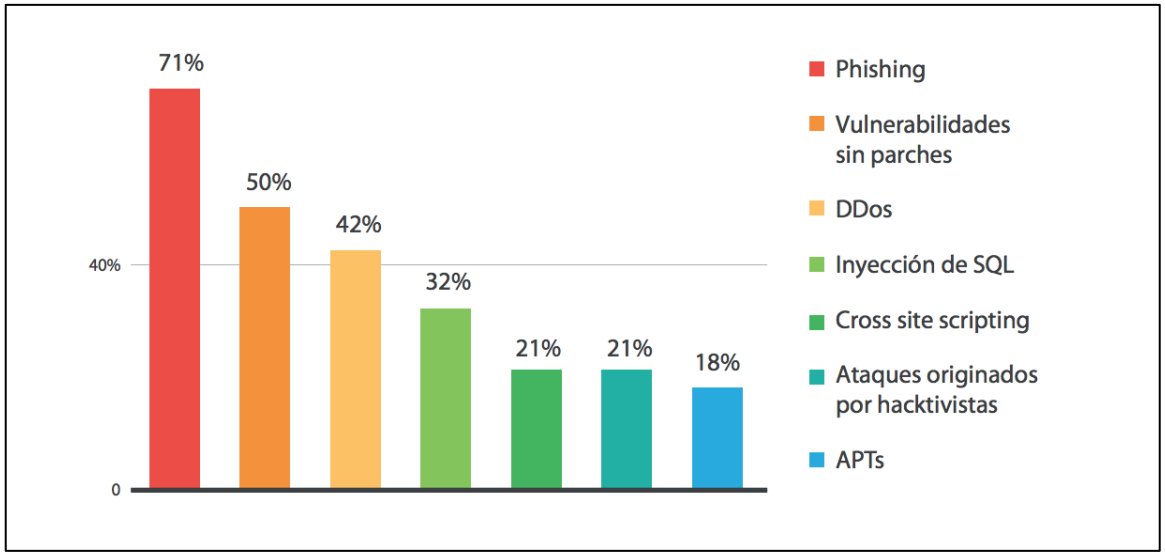
- La mayoría de las regiones en las que se aplicó la encuesta indicaron que su equipo ICS/SCADA estaba siendo atacado, lo que revela una gran cantidad de actividad por parte de los Ciberdelincuentes. Si bien muchos de estos ataques

podrían ser para reunir inteligencia sobre sus objetivos, se puede prever que más regiones reportarán esto en el futuro conforme sus infraestructuras críticas se vuelvan más conectadas o mejoren su capacidad de identificar la presencia de un ataque.

Tipos de Métodos para Ataques Cibernéticos

- ¿Qué tipo de ataques cibernéticos se han utilizado contra su organización?

Gráfica 3. Tipos de ataques realizados



Fuente: Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas [en línea]. Organization of America States, Trend Micro, 2015 [consultado 24 de Octubre de 2015]. Disponible en Internet: https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

A partir de los resultados anteriores, se observó que la mayoría de las regiones están enfrentando ataques de phishing contra sus organizaciones.

Actualmente es el phishing la primera amenaza que se utiliza en los ataques dirigidos y podría ser un indicador del estado real de las actividades relacionadas con este tipo de ataques aunque esta fue la amenaza más baja señalada en los resultados de la lista anterior. Esto también indicaría que los intentos iniciales de los atacantes es penetrar en una organización para tratar de moverse lateralmente a otros sistemas, como sus dispositivos ICS/SCADA.

Los Ciberdelincuentes a menudo utilizan vulnerabilidades que no tienen parche en sus rutinas de infección pues reconocen que la aplicación de parches es un proceso difícil para muchas organizaciones. Asimismo, muchos dispositivos de la infraestructura crítica utilizan versiones antiguas de los sistemas operativos y de las aplicaciones, y son más propensos a ser vulnerables ya que muchas ya no reciben soporte.

Como se vio con anterioridad, los ataques se están volviendo más prevalentes y sofisticados, lo que exigirá que las organizaciones estén mejor preparadas.

Percepción de la Preparación para los Incidentes Cibernéticos

- ¿Cuán preparada está su organización para un incidente cibernético?

La mayoría de los países consideran que están algo preparados para un incidente cibernético, lo cual es una buena noticia, pero los resultados de la siguiente encuesta sugieren que el esfuerzo por mejorar su preparación podría ser más complicado de lo que parece. Asimismo, el aumento en el número y sofisticación de los ataques significa que los países que no están preparados o que están algo preparados deben considerar de inmediato mejorar sus capacidades de detección, protección y respuesta.

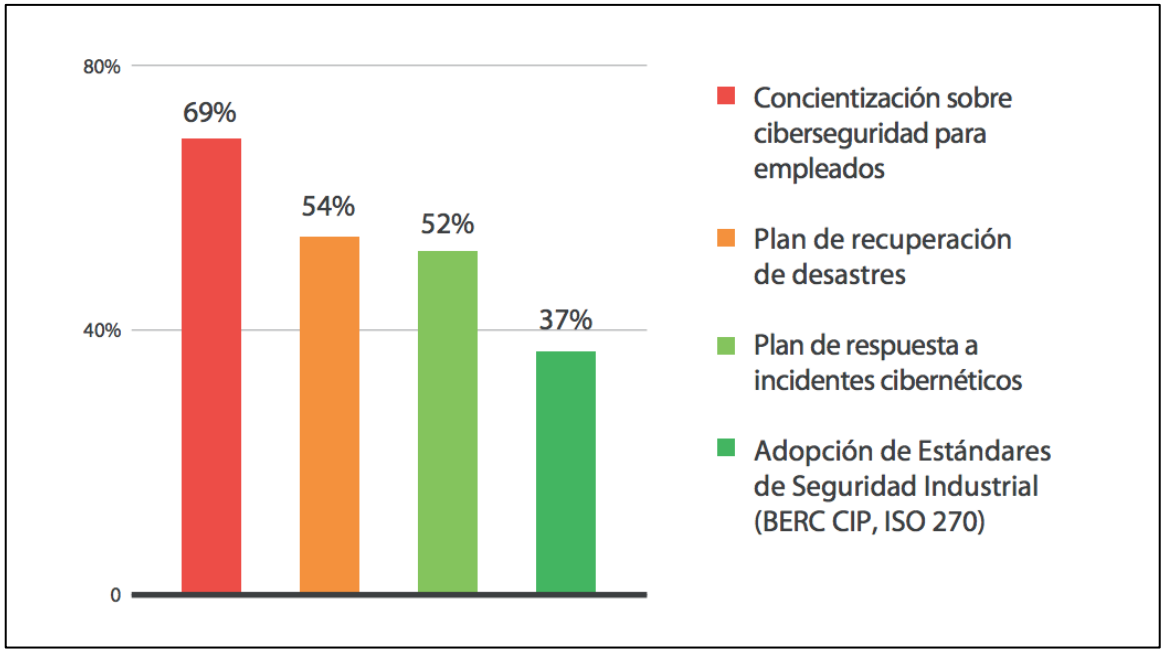
Gráfica 4. Preparación de las organizaciones

Fuente: Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas [en línea]. Organization of America States, Trend Micro, 2015 [consultado 24 de Octubre de 2015]. Disponible en Internet: https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

Políticas de Ciberseguridad

- ¿Su organización tiene políticas y/o planes de Ciberseguridad?

Gráfica 5. Planes de Ciberseguridad



Fuente: Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas [en línea]. Organization of America States, Trend Micro, 2015 [consultado 24 de Octubre de 2015]. Disponible en Internet: https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

La preparación comienza con un plan, y si únicamente poco más de la mitad (52%) de los encuestados dijeron tener un plan de respuesta a los incidentes cibernéticos, no es un buen presagio si ocurriera un incidente. No se han implementado los controles industriales (ICS/SCADA) con las medidas de seguridad necesarias y por tanto muchas regiones han añadido regulaciones y estándares para éstos. Únicamente 37% de las organizaciones han adoptado esos estándares, lo que incrementa el riesgo de comprometer sus dispositivos.

Finalmente cuando se habla de Ciberseguridad, se hace referencia a un tema que aunque amigable y familiar en concepto, no lo es del todo en profundidad. Pareciese ser que en los sectores y organizaciones de dichas áreas que se vienen cubriendo, y que son el objeto de estudio de este proyecto, el tema no se esté manejando con la importancia que tal vez este merece y las serias consecuencias que de por seguro pueden llegar a representar.

4.2 PARTE 2. CASO DE ESTUDIO: INVESTIGACIÓN DEL SECTOR DE LAS REDES DE TELECOMUNICACIONES

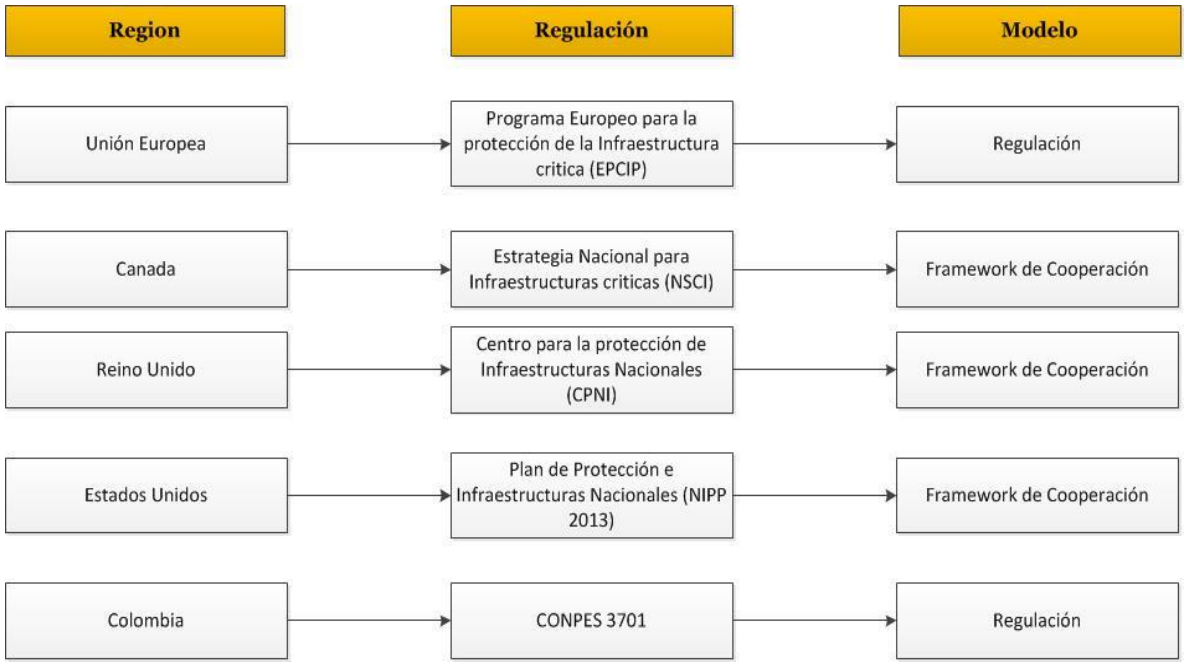
4.2.1 ¿Cuáles son las infraestructuras críticas? Aunque con anterioridad se ha hecho énfasis en este tema a lo largo de este documento, vale la pena recalcar que las Infraestructuras críticas incluyen cualquier elemento de un sistema que se requiere para mantener la función social, mantener la salud y la seguridad física, así como garantizar el bienestar social y económico de un país. Dentro de las infraestructuras críticas podemos clasificar al sector energético, los servicios públicos, los sistemas financieros, la salud y el acueducto; estos elementos mencionados con anterioridad no operan de manera aislada en la actualidad. Cada vez más, la conectividad y la dependencia entre estos sistemas aumentan la complejidad de la gestión de las infraestructuras.

Para ayudar a hacer frente a los riesgos de seguridad asociados con la complejidad y las dependencias dentro de varios sistemas de infraestructuras críticas, algunos organismos de normalización y agencias federales en al menos doce países han definido los criterios de las normas de seguridad, así como los métodos de implementación a adoptar. Por ejemplo, la Unión Europea (UE) se ha movido hacia un régimen de infraestructura crítica legislado a través del Programa Europeo para la Protección de Infraestructuras Críticas (PEPIC), Estados Unidos ha adoptado un modelo de cooperación entre el Departamento de Seguridad Nacional y la industria con los planes de protección de la Infraestructura Nacional.

En Canadá y el Reino Unido por su parte, los marcos de cooperación están en un mismo lugar a través de la Estrategia Nacional para la Infraestructura Crítica y el Centro para la Protección de la Infraestructura Nacional. Para el caso de Colombia, el documento de regulación existente es el CONPES 3701 el cual expone los lineamientos de política para Ciberseguridad y Ciberdefensa propuesto por el Ministerio de Tecnologías de la información y las comunicaciones, entre otros.

En estos ejemplos de marcos regulatorios, sólo el PEPIC legisla una respuesta de los operadores del gobierno y de los operadores de industrias de infraestructuras críticas. En el PEPIC, se especifican las obligaciones de los países de la UE y los soportes están disponibles para la adopción del PEPIC por parte de los estados miembros. En los ejemplos de - Canadá, el Reino Unido y los Estados Unidos - se emplea un marco de cooperación entre los operadores y gobierno con el fin de fomentar la comunicación de las mejores prácticas para la infraestructura crítica y las principales amenazas existentes. En cuanto a Colombia, lo propuesto en el documento mencionado con anterioridad, CONPES 3701, es el acercamiento que ha propuesto el Gobierno para afrontar la problemática que representa enfrentar amenazas Cibernéticas; previo a este documento no existía una estrategia nacional al respecto. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por las entidades involucradas directa e indirectamente con las infraestructuras críticas. A continuación, una representación gráfica en relación a lo mencionado con anterioridad, que muestra lo expuesto por cada región en cuanto a regulación y al modelo adoptado por cada una:

Gráfica 6. Marcos regulatorios



4.2.2 Amenazas a las infraestructuras críticas. A medida que la complejidad y la dependencia aumentan en las infraestructuras críticas, los proveedores de dichas infraestructuras deben hacer frente al creciente número de nuevas vulnerabilidades Cibernéticas en sus sistemas y realizar una adecuada gestión de posibles amenazas. Como se indica en el documento generado por los Estados unidos en la Estrategia Nacional para la protección física de las infraestructuras críticas y activos clave, tres efectos pueden constituir la vulnerabilidad en un sistema:

- **Efecto directo en la infraestructura:** Detención de las funciones de las infraestructuras críticas o activos clave a través de ataques directos a un nodo crítico, sistema o función.

- **Efecto indirecto en la infraestructura**: Consecuencias financieras para el gobierno, la sociedad y la economía a través de reacciones de los sectores público y privado a un ataque.

- **La explotación de la infraestructura:** Explotación de los elementos de una infraestructura concreta para interrumpir o destruir otro objetivo.

La creciente complejidad de este tipo de vulnerabilidades y amenazas hacia los sistemas, requiere la cooperación entre la industria y el gobierno. Estas tendencias existentes y emergentes conducen a un requisito para la aplicación coherente de la Ciberseguridad por las partes interesadas de la industria, los proveedores clave de la infraestructura, y el gobierno con el fin de proteger las infraestructuras críticas vital financiera, comercial, y el bienestar social.

4.2.3 Introducción a la identificación de riesgos. Hoy en día, los atacantes o Ciberdelincuentes están constantemente evolucionando y afilando sus capacidades para explotar nuevas vulnerabilidades. Identificar y abordar estas amenazas requerirá que los operadores de telecomunicaciones realicen inversiones y actividades de aproximación que generen conocimiento sobre los activos de información, amenazas y vulnerabilidades dentro de sus organizaciones.

Actualmente las organizaciones que soportan infraestructuras críticas, están iniciando un proceso de concientización que ha venido creciendo de la necesidad de controlar dichos riesgos informáticos operacionales debido a la utilización extensiva de las nuevas tecnologías, a la existencia de una infraestructura de información mundial y a la aparición de nuevos riesgos. La dependencia de los individuos, de las organizaciones y de los países, en cuanto a los sistemas de información y de las redes, constituye un riesgo de primer orden que debe contemplarse como un riesgo de seguridad.

Teniendo en cuenta lo anterior, las infraestructuras de telecomunicaciones (o cualquier infraestructura crítica) y los servicios y actividades que éstas permiten desarrollar, deben poder plantearse, concebirse, así como instalarse y administrarse en términos de seguridad; antes de realizar cualquier tipo de actividad dentro de una organización que soporta infraestructuras críticas, la seguridad debe contemplarse como una de las bases primordiales de las mismas. Sin embargo, en relación a lo inmediatamente anterior, resulta curioso que mientras que el número de ataques de seguridad contra infraestructuras críticas ha ido en aumento, según un estudio anual desarrollado por la PWC, se encontró que los ejecutivos de telecomunicaciones detectaron 17% menos de incidentes de

seguridad en los últimos 12 meses, en comparación con el año 2012. Los encuestados en dicho estudio informaron también de una disminución en los costos financieros atribuidos y relacionados a los incidentes de seguridad.

En comparación, según el mismo estudio, los incidentes de seguridad se han incrementado, teniendo en cuenta que los resultados de los encuestados, en general para todas las industrias las cuales reportan un salto del 25% en los incidentes detectados. El hecho de que las organizaciones de telecomunicaciones no estén reportando más incidentes sugiere, en parte, que los viejos modelos de seguridad en su uso pueden ser ineficaces contra los atacantes sofisticados de hoy en día. Por ejemplo, y siguiendo con esta línea de ideas, el número de encuestados que no conocen la frecuencia de los incidentes de seguridad sigue aumentando año tras año - es ahora un 19%, frente al 14% el año pasado y un 8% en 2011 - que sirve para contradecir la idea de que las organizaciones son cada vez mejores para detectar y responder a las intrusiones.

Las empresas u organizaciones del sector de las telecomunicaciones, como se ha señalado a lo largo de este documento, deberían tener debido a la criticidad de los servicios que soportan, cierta familiaridad en relación a la gestión de los riesgos de seguridad de la información; los sistemas informáticos conectados en red son recursos accesibles a distancia y blancos potenciales de ataques informáticos. Esto incrementa los riesgos de intrusión en los sistemas y ofrece un terreno favorable para la realización y propagación de ataques y delitos.

Para las organizaciones que soportan infraestructuras críticas, el tomar acciones para lograr un mayor nivel en la forma en que identifican los riesgos y las amenazas dinámicas resulta ser entonces una tarea primordial.

Se puede ver como el mostrar solidez en la identificación de riesgos, puede llegar a alinearse de cierta forma con los objetivos del Framework de Ciberseguridad de NIST, donde los objetivos del programa de Ciberseguridad de una organización están alineados con la estrategia empresarial y los gastos que esto representa para una compañía.

Así pues, las compañías que soportan infraestructuras criticas como las del sector de las telecomunicaciones y los servicios que ofrecen y soportan, plantean problemas de seguridad informática, complejos y cambiantes, que sin un proceso de gestión e identificación de riesgos definido o un programa de Ciberseguridad,

serían difíciles de controlar y que podrían traer posibles consecuencias y repercusiones críticas sobre el funcionamiento normal de dichas organizaciones.

De la capacidad de controlar los aspectos en relación a la seguridad de estas compañías, y de los procesos, los sistemas, y las infraestructuras que estas mismas soportan, dependen los factores críticos de éxito de las economías de muchas sociedades.

La consideración de realizar un análisis de identificación de los riesgos dentro de las organizaciones que soportan infraestructuras críticas, en un proceso de gestión de riesgos, inspira e impulsa en gran medida al planteamiento de estrategias de seguridad de la información y Ciberseguridad. La gestión de los riesgos constituye el punto de partida del análisis de las necesidades de seguridad, que permitirá definir la estrategia y la política de seguridad de cualquier organización, incluyendo las que soportan infraestructuras críticas.

Para cualquier organización, el control de los riesgos informáticos supone la concepción de una estrategia, la definición de una política de seguridad y su realización táctica y operacional.

4.2.3.1 Identificación de Riesgos. Para iniciar un análisis de identificación de riesgos en las empresas del área de las redes de telecomunicaciones, se debe tener en cuenta lo siguientes puntos clave:

- Identificación de los procesos críticos a nivel infraestructura y protocolos.
- Identificación de activos involucrados en estos procesos.
- Análisis de vulnerabilidades y amenazas.
- Controles existentes.

4.2.3.2 Identificación de procesos críticos a nivel de infraestructura y protocolos. Para el sector o área objeto de estudio en este documento de investigación, la disponibilidad de las comunicaciones puede llegar a ser considerada uno de los procesos más críticos, ya que una interrupción de un tiempo considerable en sus operaciones, podría tener un impacto catastrófico en la imagen corporativa, en la confianza de los clientes y usuarios de acuerdo a la mala calidad de servicio percibida ante este incidente. Dicha desconfianza e interrupción de los servicios que proveen las empresas de este sector seguramente impacte directamente otros procesos de negocio internos llegando a generar pérdidas potenciales. Cabe resaltar que para dicha disponibilidad en las comunicaciones mencionada con anterioridad se evaluaran los protocolos de comunicación que permiten el transporte y el flujo de información (IPv4 e IPv6).

4.2.3.3 Identificación de activos involucrados en los procesos críticos. Previamente a la identificación de los riesgos, se debe realizar un inventario clasificando los activos, utilizando cualquiera de los procedimientos recomendados por estándares internacionales reconocidos. Para este documento y su sector objeto de estudio, algunos puntos a tener en cuenta son:

Infraestructura, servicios y protocolos

- Backbone “Troncal” / Core “Núcleo”.

- Hardware/Dispositivos: infraestructura tecnológica de red tal (elementos activos: Routers, switches, hubs, etc. Elementos de red pasivos: Cableado estructurado, servers, Equipos de escritorio, terminales, entre otros.

- Servicios primordiales para el negocio.

- Convergencia (Entre los Protocolos y los servicios ofrecidos):

- Voz sobre IP
- Mensajería electrónica
- Datos
- Conmutación de etiquetas multiprotocolo “MPLS”
- Servicios sobre líneas de abonado digital Asimétricas “ADSL”.

Sistemas informáticos – Software. En esta área se incluyen las aplicaciones (los desarrollos internos y los realizados por terceros), el software base (los Sistemas de gestión de bases de datos, los Sistemas Operativos, etc.), los sistemas de clasificación de recursos empresariales “ERP’s”, etc. También se debe tener en cuenta el software de control y gestión de operaciones específicas, los analizadores de tráfico y protocolos, el monitoreo de la red, etc.

Teniendo en cuenta el crecimiento exponencial que ha tenido el uso de internet en los últimos años (tendencia a los servicios basados en el protocolo IP con protocolos como IPv4 e IPv6), así como el gran auge de los servicios online y el impulso que esto le ha dado al desarrollo económico nacional, aparecen nuevas amenazas relacionadas con el uso de estos protocolos mencionados con anterioridad.

4.2.4 Análisis de vulnerabilidades y Amenazas. Es muy importante al momento de identificar amenazas, entender que las mismas deben clasificarse según su naturaleza. Una vez hecho esto, de igual forma es importante mantenerse actualizado constantemente en cuanto a los 0 day (ataques de día cero) y los APTs (Amenazas persistentes avanzadas) que aparecen como nuevas amenazas.

En la recomendación realizada por la ITU en el documento ITU-T Rec. X.800, se propone un marco de seguridad, el cual puede llegar a aplicarse a este caso de estudio para el sector de las telecomunicaciones. Según lo descrito en dicha

recomendación, las entidades u organizaciones que pertenezcan al sector de las telecomunicaciones, deberán implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso. Se puede observar a continuación, las posibles amenazas:

- Destrucción de los activos de información.
- Violación de la integridad de la información.
- Pérdida de la disponibilidad de la información.
- Pérdida de la confidencialidad de la información.
- Denegación de los servicios.

De igual forma, en la Recomendación X.800, se detallan los aspectos referentes a modelos de seguridad a tener en cuenta por parte de dichas entidades, y que tienen que ver con el dimensionamiento de la seguridad de la información en cuanto a la autenticación, acceso, servicio de no repudio, principio de confidencialidad de datos, principio de integridad de datos y principio de disponibilidad.

Cabe resaltar entonces, que para los riesgos relacionados con los protocolos de internet mencionados con anterioridad, es decir, para los protocolos IPv4 e IPv6, y que se encuentran relacionados directamente con las entidades u organizaciones del sector de las telecomunicaciones, podemos ver los siguientes tipos de posibles amenazas.

Por ejemplo, amenazas que deben ser consideradas en IPv6:

- Escaneo de debilidades en Gateway y Hosts.
- Escaneo de direcciones Multicast.

- Control de acceso no autorizado.

- Ataques a Firewalls.

- Debilidades en los protocolos.

- Denegación de servicios (DDOS).

- Virus y gusanos informáticos (ya existen algunos virus para IPv6 como Rbot, DUD, etc.

También es importante conocer los motivos de las posibles vulnerabilidades y amenazas en escenarios internos.

Es importante mencionar, que otro elemento importante que puede resultar de gran ayuda para la comprensión de amenazas, es el análisis de los posibles vectores de ataque a los que se encuentran expuestos.

A continuación se mencionan algunos tipos de vulnerabilidades y ataques presentes en estos protocolos de internet:

- **Ataques automatizados**, como "*Ataque SLAAC*", o el ataque de auto configuración de direcciones sin estado. La versión actualizada del SLAAC, llamado "*sudden six*", que establece un ataque man-in-the-middle en conexiones que no tienen habilitado el protocolo SSL y que podría ser aprovechada para atacar incluso sesiones protegidas por dicho protocolo dependiendo de cómo la sesión SSL se establezca.

- **Vulnerabilidades en IPSec:** Si bien es cierto que el protocolo IPv6 trae consigo algunos y nuevos aspectos, como IPSec integrada y mayor efectividad al tratar de mapear una red mediante un escaneo tradicional, es importante tener en cuenta que la adopción de dicho protocolo trae consigo nuevos riesgos y amenazas inherentes a su implementación, como los son ataques de inyección SQL y XSS (dirigidos a las aplicaciones web), así como difusión de malware y robo de datos.

- **Vulnerabilidades en Firewalls:** Una posible consecuencia de la implementación de IPv6 puede verse en el momento de dejar la red expuesta al ingreso indiscriminado de paquetes provenientes del exterior y desde cualquier host en internet. Dependiendo de la estructura o arquitectura de red escogida, el administrador de una red podría optar por una, donde según las reglas determinadas en el firewall, sólo se permita el tráfico entrante *si este proviene como respuesta a solicitudes originadas desde la red interna*. Lo recomendable seria entonces proteger las subredes basadas en IPv6 a través de un *firewall de estado* que sólo permita tráfico de retorno. De esta forma, y al menos en cuanto a materia de filtrado de paquetes, las arquitecturas de subredes en el protocolo IPv6 no serán diferentes del de una subred basada en el protocolo típico IPv4.

- **Ataques mediante escaneo de direcciones IP**: Lo recomendable seria implementar en el perímetro del esquema de red de la organización, y al igual que lo mencionado en el punto anterior, un Firewall de estado que únicamente permita el tráfico que viene en respuesta a las solicitudes generadas desde la red interna (tráfico de retorno). De esta forma conseguir, que en caso de que llegase a presentarse un posible ataque, los paquetes enviados por el atacante nunca lleguen hasta los hosts que hacen parte de la arquitectura de la red.

- **Ataques de fuerza bruta**: Los ataques de escaneo de direcciones IPv4 mediante la fuerza bruta, y que en algún punto se han convertido en comunes o habituales, se debe al limitado espacio existente de direcciones que caracteriza a dicho protocolo y que de una forma u otra, facilita un escaneo de fuerza bruta por parte del atacante. Viéndolo desde este punto de vista, y al saber que el protocolo de internet IPv6 viene con diferentes características, los ataques de escaneos de direcciones para dicho protocolo IPv6 podrían a llegar a ser de alguna forma más fundamentados que los ya conocidos para el protocolo de IPv4. Sobre IPV6, los atacantes podrían llegar a emplear métodos o estrategias de reconocimiento de red, mediante la identificación de posibles hosts vulnerables a ataques, usando direcciones IPv6 filtradas.

4.2.5 Controles existentes. Como se pudo observar en el anterior segmento, donde se planteaba la relación existente entre los riesgos de Ciberseguridad y los riesgos en los protocolos de internet, IPv4 e IPv6, se deben abordar de igual forma, los controles que pueden llegar a derivarse de dichos riesgos, y que de alguna forma puedan llegar a reducir las vulnerabilidades identificadas.

Es importante poder armonizar los planes de tratamiento de riesgos de las empresas del sector de las telecomunicaciones con los controles que puedan llegar a identificarse. Es decir, que en realidad dichos controles tengan o puedan llegar a tener el efecto y los resultados deseados al relacionarlos a sus respectivos riesgos. De esta forma, se obtendrán los elementos necesarios para un mejor análisis y evaluación de los riesgos reales dentro de la organización, y un uso apropiado de las inversiones en seguridad, llegando a priorizar con mayor certeza los objetivos a los que se les quiera dar prioridad.

Cabe aclarar, que al igual que se da con otras áreas de vital importancia, la investigación en temas de seguridad presenta una ardua tarea debido a la falta de información en cuanto a Ciberseguridad, ya sea por desconocimiento de los mismos, o por temas de índole confidencial; en algunas ocasiones, las investigaciones logran proveer información relevante a las organizaciones durante el proceso de identificación de riesgos. Debido a la criticidad de las operaciones y de la información que manejan dichas compañías que pertenecen a sectores críticos, la información acerca de los controles utilizados puede llegar a ser de difícil acceso.

A continuación se expone una breve descripción de algunos controles a considerar en el caso de una organización del sector de las redes de telecomunicaciones.

4.2.5.1 Controles Capa Núcleo

- **Integridad de los elementos de red:** En caso dado que uno de los dispositivos de red deje de funcionar, el flujo de la red debe de mantenerse y enrutarse nuevamente hacia un dispositivo diferente para mantener el servicio. Aquí entraría en juego el concepto de redundancia junto con el de alta disponibilidad para los dispositivos del Core de la red.

- Autenticación de rutas.

4.2.5.2 Controles Capa de distribución

- Verificación de la Integridad de dispositivos y la disponibilidad de los elementos red.

- Autenticación de rutas.

- Firewall stateful: Filtrado dinámico de paquetes, inspección de las capas 3 y 4 del modelo OSI.

- Firewall stateless: Filtra y examina los paquetes IP independientemente, lo cual corresponde al nivel 3 del modelo OSI.

- Métodos de cifrado en canales de comunicación.

- Confidencialidad de las comunicaciones para prevenir la interceptación de comunicaciones no autorizadas.

- Controles sobre suplantación de identidad (arp spoofing, email spoofing, web spoofing).

- Controles para contrarrestar ataques de denegación de servicio (DDos).

- Controles para contrarrestar ataques de distribución de negación de servicio (DDos).

- Controles sobre botnets y APT (Advanced persistent threats).

4.2.5.3 Controles Capa de Acceso

- Controles de seguridad sobre Routers:
  - ♦ Guías de hardening.
  - ♦ Cambios de Configuraciones por defecto.
  - ♦ Listas de control de acceso (ACLs).
- Monitoreo de seguridad:
  - ♦ IDS (sistema de detección de intrusos).
  - ♦ IPS (sistema de prevención de intrusos).
  - ♦ Firewalls.
  - ♦ WAF (web application firewall).
  - ♦ Políticas de gestión de listas negras de correos, navegación, spam, pishing, etc.
  - ♦ Gestión de logs y monitoreo (autenticación de usuarios para accesos a dispositivos de red y servidores).

5. FRAMEWORK DE CIBERSEGURIDAD DE NIST

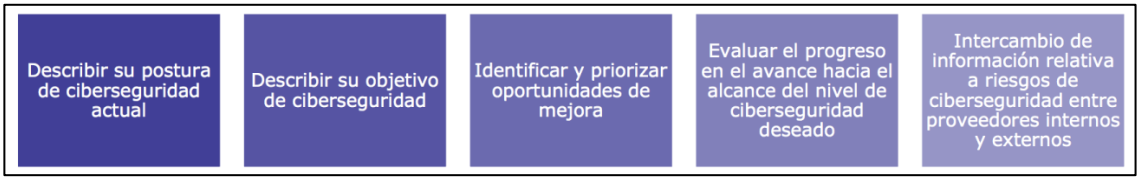
A continuación en este documento de investigación, se dará un vistazo a nivel general sobre el Framework de Ciberseguridad desarrollado por NIST, sus principios teóricos y fundamentos principales, es decir, la base que compone a dicho Framework, sin embargo no se entrará en detalle dentro de los conceptos más profundos y específicos del mismo. En caso de que el deseo del lector sea profundizar un poco más acerca de cada una de las etapas del Framework que se describirán a continuación, puede remitirse al documento oficial generado por NIST o al capítulo expuesto más adelante en este mismo documento donde se encuentra una explicación un poco más detallada.

5.1 INTRODUCCIÓN AL FRAMEWORK

Debido al incremento de amenazas internas y externas, las organizaciones responsables de infraestructuras críticas y los modelos de negocios que representan, deben tener un enfoque consistente e iterativo al momento de evaluar y gestionar sus riesgos de Ciberseguridad.

Como se mencionó en la introducción al Marco Teórico en este documento de investigación, para febrero del año 2014, NIST desarrolló en colaboración con la industria Norte Americana, un Framework de Ciberseguridad con el objetivo de proveer una orientación más clara en la gestión de riesgos de Ciberseguridad de aquellas organizaciones o empresas que soportan infraestructuras críticas. Básicamente el Framework de Ciberseguridad elaborado por NIST, comprende una estructura que guía y orienta a las organizaciones a realizar los siguientes procedimientos:

Gráfica 7. Mecanismo guía del Framework

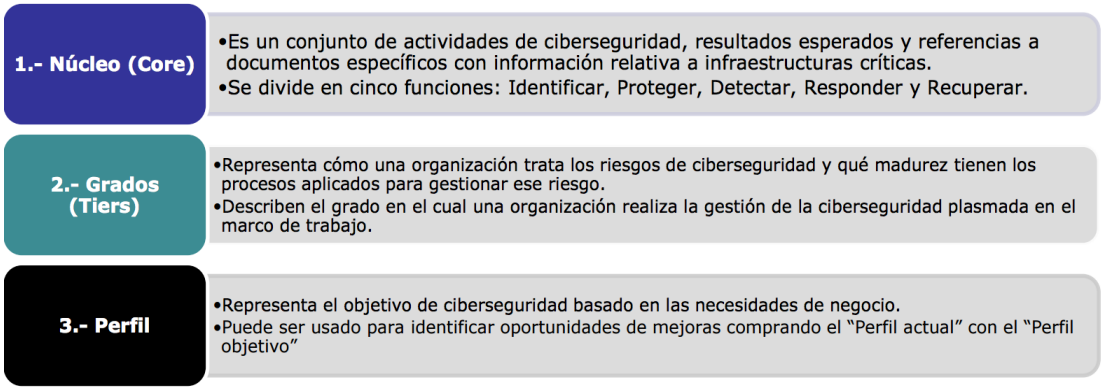


Fuente: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas [en línea]. SCADALAB, 2014 [Consultado 8 de enero de 2015]. Disponible enInternet:http://www.infoplc.net/files/documentacion/ciberseguridad/infoPLC_net_SCADALAB_Modulo_2_Tema_2.pdf

Se puede observar partiendo de la estructura anterior, que el enfoque del Framework está basado en la gestión de los riesgos de Ciberseguridad. La gestión del riesgo es el proceso continuo basado en: identificar, evaluar y responder a los riesgos. Por su parte, la evaluación de los mismos es el proceso mediante el cual se sabe cómo enfrentar y tratar los riesgos previamente identificados. Con la comprensión y evaluación de los riesgos, las organizaciones pueden informar y dar prioridad a las decisiones en cuanto a lo que concierne a la Ciberseguridad.

A continuación se describe la estructura del Framework, la cual incluye cada una de sus tres partes básicas o fundamentales. Estas están compuestas por el Núcleo, los Niveles (Tiers) y el Perfil del Framework:

Gráfica 8. Estructura del Framework



Fuente: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas [en línea]. SCADALAB, 2014 [Consultado 8 de enero de 2015]. Disponible enInternet:http://www.infoplc.net/files/documentacion/ciberseguridad/infoPLC_net_SCADALAB_Modulo_2_Tema_2.pdf

5.1.1. El Núcleo (Core). Este elemento del Framework conocido y documentado en diversos textos solo como el "Core" está organizado en:

- **Funciones:** son las actividades que se desarrollarán a lo largo del Framework, y están divididas en: Identificar, Proteger, Detectar, Responder y Recuperar.

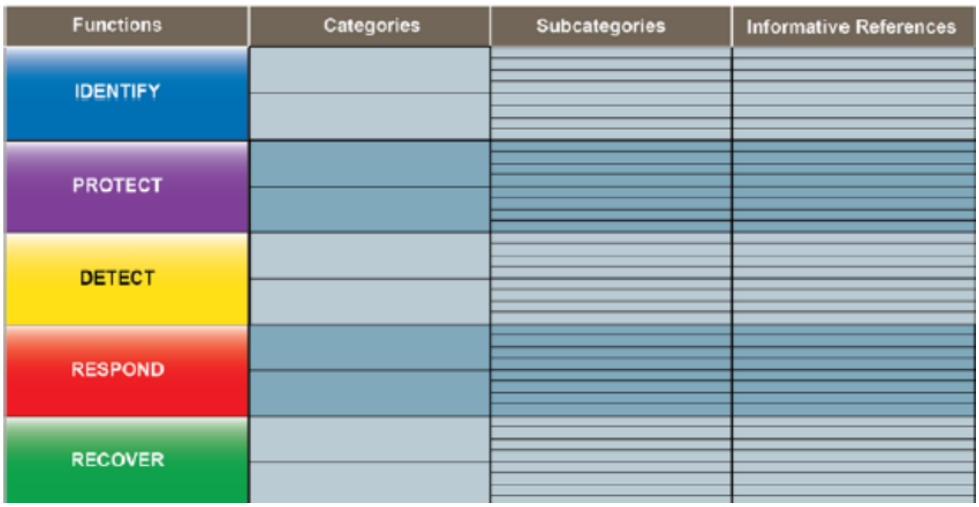
- **Categorías:** son las subdivisiones de las funciones. Algunos ejemplos de estas categorías son: Gestión de activos, Seguridad en los datos, Control de acceso, Monitoreo continuo de la seguridad, Mitigación, Plan de recuperación (o respuesta a incidentes), etc.

- **Subcategorías:** son las acciones que ayudan a que cada objetivo de las categorías se cumplan. Por ejemplo: para la categoría Gestión de activos, una de sus subcategorías sería "los dispositivos físicos y sistemas dentro de la organización deberán estar inventariados", y así con cada una de las categorías que puede tener una o más subcategorías.

- **Referencias informativas:** en esta sección se ven las referencias a las guías de buenas prácticas y a los estándares de seguridad que buscan proponer un método para alcanzar cada objetivo de las subcategorías.

Para efectos ilustrativos, a continuación la representación gráfica de la distribución de los elementos que componen el Núcleo.

Gráfica 9. Funciones del Framework



Fuente: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas [en línea]. SCADALAB, 2014 [Consultado 8 de enero de 2015]. Disponible enInternet:http://www.infoplc.net/files/documentacion/ciberseguridad/infoPLC_net_SCADALAB_Modulo_2_Tema_2.pdf

Para un mejor entendimiento del Núcleo, se describirán cada una de las funciones que hacen parte de su estructura:

- **Identificar (Identify):** Desarrollar la comprensión de la organización para gestionar el riesgo de Ciberseguridad aplicado a los sistemas, activos, datos y capacidades.

- **Proteger (Protect):** Desarrollar y poner en práctica las acciones adecuadas para garantizar la integridad de la infraestructura crítica.

- **Detectar (Detect):** Desarrollar y poner en práctica las actividades pertinentes para detectar la ocurrencia de un evento de Ciberseguridad.

- **Responder (Respond):** Desarrollar e implementar las actividades necesarias para adoptar medidas respecto a la sucesión de un evento de Ciberseguridad detectado.

- **Recuperar (Recover):** Desarrollar e implementar las actividades necesarias para mantener los planes que permitan restaurar los servicios que fueron perjudicados debido a un evento de Ciberseguridad así como la propia continuidad del negocio.

5.1.2 Niveles (Tiers). Este elemento del Framework proporciona información acerca del contexto sobre cómo una organización entiende los riesgos de Ciberseguridad y los procesos que tiene establecidos en la actualidad dentro de su programa de gestión del riesgo (en caso de que tenga alguno) para gestionarlos.

Para desarrollar los Tiers, las empresas u organizaciones deben:

- Determinar el Estado “actual” en el cual se encuentran (basándose en cada uno de los Tiers: Parcial, Riesgo conocido, Repetible o Adaptativo) y escoger en cuál de ellos encaja mejor su nivel de Ciberseguridad actual.

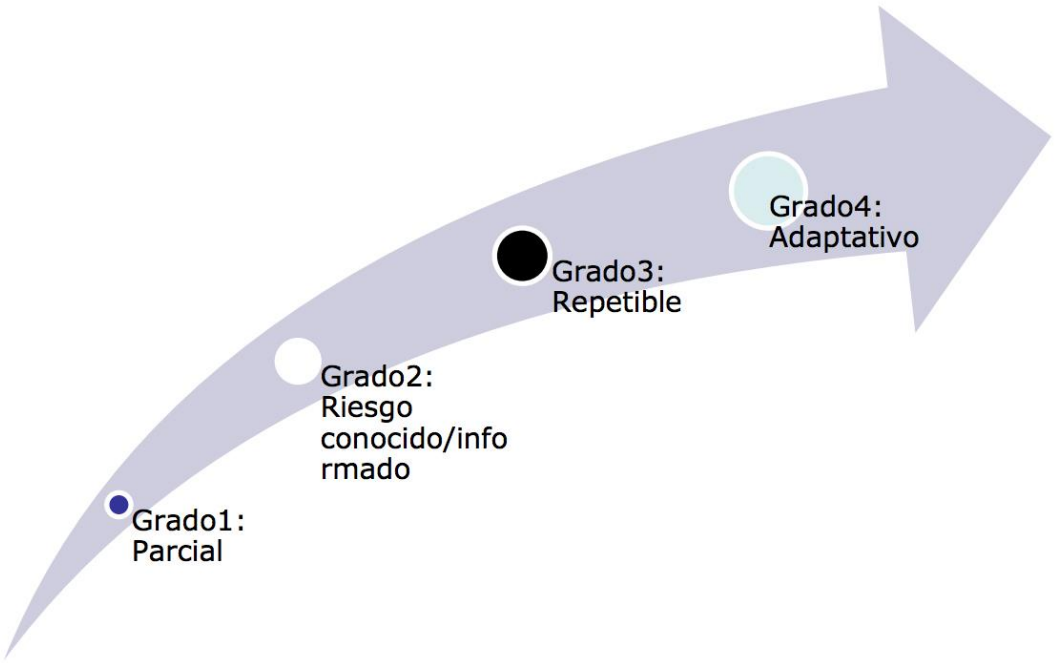
- Determinar el Estado “deseado” al cual quieren llegar, asegurando que el nivel seleccionado cumple con los objetivos de la empresa, es factible de implementar, y reduce el riesgo de la Ciberseguridad para los activos críticos y recursos a un nivel aceptable para la organización.

Debe tenerse en cuenta, que una organización puede alinear la aplicación de los Tiers con el alcance deseado para el uso del Framework mismo. Por ejemplo, si una organización decide utilizar el Framework sólo para una unidad de negocio o

un proceso específico, los Tiers podrían ser utilizados para describir la solidez o robustez global de los procesos de la gestión de riesgos en esa unidad de negocio o el nivel de dicho proceso específico.

En la siguiente grafica se observan los Tiers o Niveles que pueden llegar a desarrollarse en una empresa u organización:

Gráfica 10. Tiers (Grados o Niveles del Framework)



Fuente: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas [en línea]. SCADALAB, 2014 [Consultado 8 de enero de 2015]. Disponible enInternet:http://www.infoplc.net/files/documentacion/ciberseguridad/infoPLC_net_SCADALAB_Modulo_2_Tema_2.pdf

- **TIER 1 – Parcial**

  - **Proceso de Gestión de Riesgos**: Las prácticas de la organización de gestión de riesgos de Ciberseguridad no están formalizados, el riesgo se gestiona de manera reactiva en algunas ocasiones.

  - La priorización de las actividades de Ciberseguridad no puede ser establecida directamente a través de los objetivos organizacionales de riesgo, el entorno de amenazas, o requisitos de negocio.

  - Se tiene un conocimiento limitado del riesgo de Ciberseguridad a nivel organizacional.

  - No existe un enfoque que tenga en cuenta a toda la organización para la gestión de riesgos de Ciberseguridad.

  - En términos de Ciberseguridad, podrían no tener procesos dispuestos para coordinar o colaborar con otras entidades.

- **TIER 2 – Riesgo conocido**

  - Las prácticas de gestión de riesgos están aprobadas por la dirección, pero no están establecidas a través de toda la organización.

  - La priorización de las actividades de Ciberseguridad están basadas en los objetivos organizacionales de riesgo, entorno de amenazas, o los requerimientos del negocio.

  - Existe una concientización de los riesgos de Ciberseguridad a nivel organizacional.

  - Los procesos y procedimientos están definidos e implementados.

- La organización no ha formalizado capacidades para compartir información externamente.

- **TIER 3 – Riesgo conocido y repetible**

  - Las prácticas de gestión de riesgos son aprobadas y documentadas formalmente.

  - Existe un enfoque que tiene en cuenta a toda la organización para la gestión de riesgos de Ciberseguridad.

  - Las políticas y procedimientos están definidas, implementadas y revisadas.

  - Las prácticas de Ciberseguridad se actualizan en base a los procesos de gestión de riesgos ya formalizados.

  - La organización colabora con aliados de negocios estratégicos y entidades externas.

- **TIER 4 – Adaptativo**

  - Al igual que en el Tier 3 existe un enfoque que tiene en cuenta a toda la Organización con la diferencia que ahora forma parte de la cultura de esta.

  - Las políticas están formalizadas basadas en los riesgos, procesos y procedimientos.

  - Las prácticas de Ciberseguridad se adaptan en base a las lecciones aprendidas y los indicadores predictivos, responde a las amenazas cambiantes en forma oportuna.

  - Se realizan mejoras continuas incorporando las tecnologías y prácticas de Ciberseguridad avanzada: el conocimiento de las actividades anteriores y actuales de los sistemas y redes.

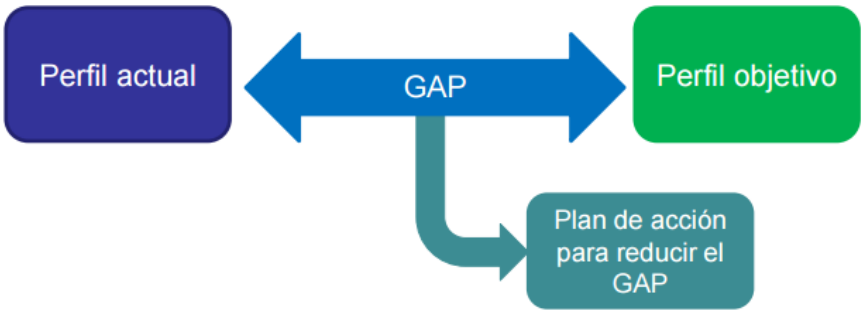
- Se comparte activamente información con los socios y aliados de negocio estratégicos para mejorar la Ciberseguridad antes de que ocurra un evento.

5.1.3 El perfil del Framework. Para este elemento del Framework, la organización define los perfiles. Dichos perfiles, pueden ser usados para describir el estado de madurez actual y el estado de madurez objetivo en las distintas actividades del Framework.

El objetivo principal de esta comparación entre perfiles (perfil actual y perfil objetivo) es revelar las lagunas o brechas que deben abordarse para lograr los objetivos de gestión de riesgos de seguridad cibernética.

En la gráfica a continuación se observa la representación gráfica del concepto mencionado con anterioridad:

Gráfica 11. Perfiles del Framework



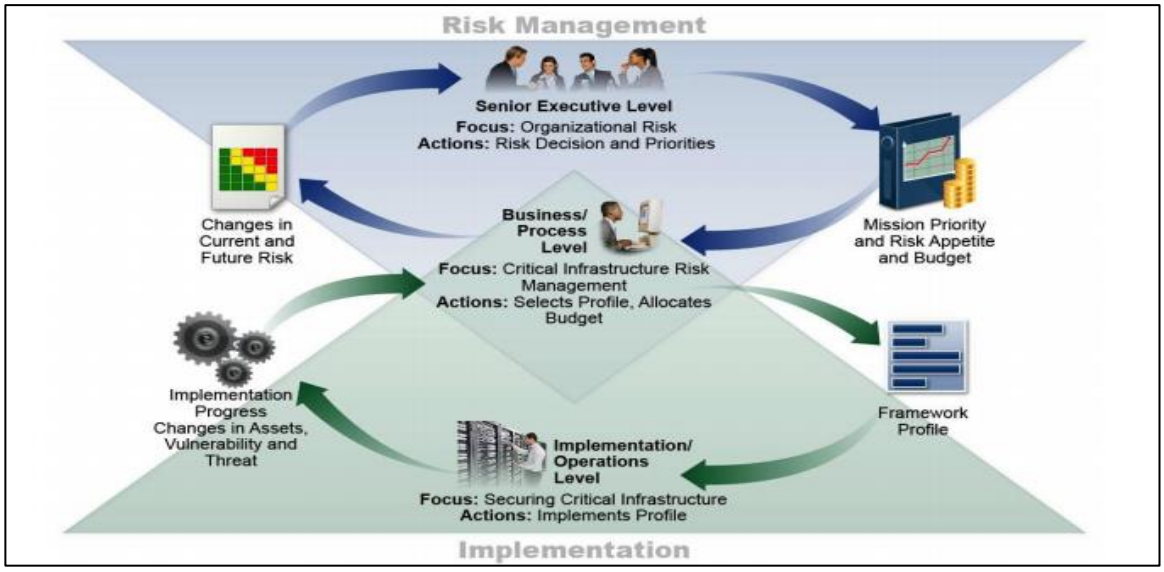
Fuente: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas [en línea]. SCADALAB, 2014 [Consultado 8 de enero de 2015]. Disponible enInternet:http://www.infoplc.net/files/documentacion/ciberseguridad/infoPLC_net_SCADALAB_Modulo_2_Tema_2.pdf

Adicionalmente el Perfil del Framework permite alinear las Funciones y Categorías con:

- Los requerimientos y metas del negocio.
- Tolerancia al riesgo.
- Recursos disponibles.
- Los requisitos legales / regulatorios.
- Mejores prácticas de la industria

La siguiente gráfica la cual fue extraída directamente del Framework de Ciberseguridad desarrollado por NIST, muestra cómo se maneja la toma de decisiones dentro de una organización para la creación e implementación del Perfil:

Gráfica 12. Flujo de información y de toma de decisiones dentro de una organización



Fuente: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas [en línea]. SCADALAB, 2014 [Consultado 8 de enero de 2015]. Disponible enInternet:http://www.infoplc.net/files/documentacion/ciberseguridad/infoPLC_net_SCADALAB_Modulo_2_Tema_2.pdf

En la gráfica se observa cómo se desarrolla y se maneja el flujo de la información dentro de la organización y su respectiva toma de decisiones a nivel jerárquico. Dentro de dicha jerarquía se pueden observar los siguientes niveles:

- **Ejecutivo (Senior Executive**), a la altura de la gestión del riesgo (Risk Management), enfocado en el riesgo organizacional.

- **Procesos de negocio (Business/Process**), cuyo foco está centrado en el manejo del riesgo de la infraestructura critica.

- **Implementación y Operación (Implementation/Operations)**, enfocado en la implementación y aseguramiento de la infraestructura crítica.

En un vistazo a nivel general del flujo allí descrito, se puede ver que: el alto nivel (ejecutivo) comunica al nivel de Procesos de negocio las prioridades de la misión, los recursos disponibles y la tolerancia global de riesgo a nivel empresarial y de proceso. El nivel de Procesos de negocio (Business/Process) utiliza dicha información como entradas en sus procesos de gestión de riesgo y colabora con el nivel de Implementación y Operación para crear el Perfil. Dicho nivel a su vez comunica la puesta en práctica o implementación del Perfil con el nivel de Procesos de negocio, quienes utilizan esta información para realizar una evaluación del impacto. Una vez obtenidos los resultados de dicha evaluación, el nivel de Procesos de negocio, lo reporta a nivel ejecutivo para informar el proceso de gestión del riesgo global de la organización. Vale la pena mencionar que como se ilustra en la gráfica anterior, el flujo de la información allí descrito es cíclico, y requiere de un monitoreo continuo como un paso crítico. Finalmente, se puede ver como después de que una organización ha identificado y definido el Núcleo (Core), los Niveles (Tiers) y el Perfil, puede llegar a implementar el Framework teniendo en cuenta los pasos:

Gráfica 13. Pasos que componen el Framework de Ciberseguridad

Fuente: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas [en línea]. SCADALAB, 2014 [Consultado 8 de enero de 2015]. Disponible enInternet:http://www.infoplc.net/files/documentacion/ciberseguridad/infoPLC_net_SCADALAB_Modulo_2_Tema_2.pdf

6. GUÍA DE REFERENCIA PARA EL ESTUDIO DE CIBERSEGURIDAD EN EMPRESAS DEL SECTOR DE LAS REDES DE TELECOMUNICACIONES BASADO EN EL FRAMEWORK DE CIBERSEGURIDAD DE NIST

6.1 CONTEXTUALIZACIÓN

En Febrero de 2014 el Instituto Nacional de Estándares y Tecnología (NIST) lanzó un Framework de implementación voluntaria enfocado a mejorar la postura en cuanto a materia de Ciberseguridad de Infraestructuras críticas con el propósito de proporcionar a las organizaciones un lenguaje o idioma común que pueda ser utilizado para evaluar y gestionar los riesgos de Ciberseguridad. Desarrollado en Estados Unidos como respuesta a la Orden Ejecutiva (EO) 13636 "*Mejora de Infraestructuras Críticas de Ciberseguridad*" de febrero de 2013, el Framework desarrollado por NIST, recomienda procesos de gestión de riesgos que permitan a las organizaciones informar y priorizar decisiones relacionadas a la Ciberseguridad con base en las necesidades del negocio sin otros requisitos de índole regulatoria o reglamentaria. Esto permite a las organizaciones, independientemente de su sector, tamaño, grado de riesgos o sofisticación en Ciberseguridad, aplicar los principios y prácticas eficaces de gestión de riesgos que mejoren la seguridad y robustez de las infraestructuras críticas. El Framework desarrollado por NIST, está diseñado para *complementar*, más no para sustituir o limitar, el proceso de gestión de riesgos de una organización ya existente y su respectivo programa de Ciberseguridad. Cada sector y organización puede llegar a utilizar el Framework adaptado a sus propias necesidades de negocio para hacer frente a sus objetivos de Ciberseguridad.

En Colombia el Ministerio de Tecnologías de la Información y las Comunicaciones, en conjunto con el Ministerio de Defensa, han comenzado a plantear una visión referente a temas de Ciberseguridad plasmados en el documento CONPES 3701, el cual busca generar los lineamientos nacionales de política en Ciberseguridad y Ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. De este marco específicamente se toma como referencia la resolución del CRC (Comisión de Regulación de Comunicaciones) 2258 del año 2009 en la cual se establecieron las características generales que se deben cumplir para garantizar la seguridad de las redes y la integridad de los servicios en las compañías que pertenecen al sector de las telecomunicaciones en Colombia.

Es entonces, como las organizaciones del sector de las telecomunicaciones en Colombia han venido presentando a través de los años, una transformación paulatina en cuanto a su postura frente a la gestión de riesgos de la Ciberseguridad, y adaptándose al mismo tiempo a las nuevas tendencias y estándares internacionales.

Esta guía de referencia para la implementación del Framework de NIST, está diseñada para asistir a las organizaciones del sector de las telecomunicaciones en:

- Caracterizar o definir su postura en Ciberseguridad actual y su objetivo relacionado con dicha postura.

- Identificar las brechas en sus programas existentes de gestión de riesgos de Ciberseguridad utilizando el Framework como guía, e identificar las áreas donde las prácticas actuales puedan llegar a exceder al Framework.

- Demostrar y comunicar efectivamente su enfoque en gestión de riesgos de Ciberseguridad, y el uso del Framework a los interesados internos y externos.

Adicionalmente en esta guía, se podrá encontrar lo siguiente: la sección 2 ofrece terminología clave del Framework de NIST y los conceptos generales básicos para su posible aplicación. La sección 3 identifica ejemplos de los recursos que podrían apoyar el uso del Framework. Por último, la sección 4 esboza un enfoque general que puede llegar a ser usado como una posible aplicación e implementación del Framework.

6.2 PREPARÁNDOSE PARA LA IMPLEMENTACIÓN DEL FRAMEWORK

Esta sección será de ayuda en la preparación de una posible implementación del Framework de Ciberseguridad de NIST orientado al sector de las telecomunicaciones, mediante la presentación de la terminología clave del Framework, así como sus conceptos y beneficios.

6.2.1 Terminología guía del Framework. Los tres componentes principales del Framework a tener en cuenta para su desarrollo e implementación son:

- El Núcleo (Core).
- Los Niveles (Tiers).
- El Perfil.

Estos términos mencionados con anterioridad se utilizan con frecuencia en este documento guía y se definen a continuación de forma un poco más amplia.

Para la descripción del **Núcleo** debe entenderse que este es: "*Un conjunto de actividades de Ciberseguridad, resultados deseados, y referencias informativas aplicables que son comunes en todos los sectores de infraestructuras críticas.*" El Núcleo está compuesto por cuatro elementos principales: Funciones, Categorías, Subcategorías y Referencias informativas.

- **Las Funciones** proporcionan (en un nivel alto), la visión estratégica del ciclo de vida de la gestión de la Ciberseguridad en una organización. Como ya se ha visto previamente en este documento, existen cinco funciones: *identificar, proteger, detectar, responder* y *recuperarse*. Cada función se divide en *Categorías, que a su vez se dividen en Subcategorías* que están acompañadas por *Referencias informativas.*

- **Las Categorías** son los resultados de Ciberseguridad que están estrechamente ligados a las necesidades programáticas y actividades particulares.

- **Las subcategorías** son los resultados concretos de las actividades técnicas y/o de gestión que apoyen el logro de cada Categoría definida con anterioridad.

- **Las Referencias informativas** son los estándares intersectoriales específicos, directrices y prácticas efectivas que ilustran un método para lograr los resultados asociados a cada subcategoría definida con anterioridad.

Los Niveles describen el enfoque que posee una organización para afrontar el "riesgo de Ciberseguridad y los procesos para gestionar ese riesgo", estos van desde el Nivel 1 (*Parcial*) al Nivel 4 (*Adaptativo*). Cada nivel demuestra un creciente grado de rigor, la sofisticación de la gestión de riesgos de Ciberseguridad y la integración con las necesidades globales de la organización; la progresión a los niveles superiores se da cuando dicho cambio sería rentable al reducir el riesgo de la Ciberseguridad.

Los Niveles están asociados con la “robustez” general del proceso de gestión de riesgos de una organización y no están ligados a las funciones, categorías o subcategorías. Una organización puede alinear la aplicación de los Niveles con el alcance deseado para el uso del Framework, por ejemplo, si una organización decide utilizar el Framework sólo para una unidad de negocio o un proceso específico, los Niveles podrían ser utilizados para describir la solidez o robustez global de los procesos de la gestión de riesgos en esa unidad de negocio o el nivel de dicho proceso especifico.

Cabe resaltar que durante el proceso de selección del nivel, una organización debería considerar sus prácticas de gestión de riesgos actuales, amenazas en el medio ambiente, los requisitos legales y reglamentarios, los objetivos/misión del negocio, y las limitaciones de la organización.

Por último los Perfiles, quienes alinean los elementos centrales del Framework con los requerimientos del negocio, tolerancia al riesgo y los recursos de la organización. El perfil puede ser utilizado para identificar oportunidades de mejora en la postura de Ciberseguridad de una organización, mediante la comparación de un Perfil actual (current profile) con un Perfil objetivo (target profile); los Perfiles proporcionan una ruta guía para reducir el riesgo de Ciberseguridad que sea coherente con las prácticas comerciales.

6.2.2 Conceptos de orientación del Framework. El objetivo central de este documento es guiar a las organizaciones que soportan infraestructuras críticas del sector de las telecomunicaciones, independientemente del nivel de madurez en que se encuentren sus programas de gestión de riesgos de Ciberseguridad (en caso de que cuenten con uno).

Para dicha orientación, las organizaciones deben tener en cuenta lo siguiente:

- **Organizaciones que no cuentan con un sistema de gestión de riesgos de Ciberseguridad:** Esta guía de implementación ayudará a ejecutar directamente el Framework o la selección de un enfoque alternativo (como un conjunto ampliamente utilizado de normas o herramientas de seguridad y gestión de riesgos) que implemente efectivamente el Framework para su respectivo uso.

- **Organizaciones que cuentan con un sistema de gestión de riesgos de Ciberseguridad:** Esta guía ayudará en la revisión de su programa existente, identificando las posibles brechas de Ciberseguridad y de gestión de riesgos. De igual forma ayudará a la alineación de su programa existente con los elementos clave del Framework propuesto.

Debe tenerse en cuenta que para utilizar el Framework en una organización, no necesariamente tienen que coincidir directamente todos los elementos de sus respectivos programas de gestión de riesgos de Ciberseguridad (en caso de que exista tal programa) con los elementos descritos en el Framework. Sin embargo, para las organizaciones que desean demostrar su alineación con el Framework, se recomienda revisar y documentar la alineación de dicho programa con los objetivos de las funciones básicas del *Framework,* así como con los *Niveles,* y los *Perfiles*.

El importante mencionar que adicionalmente el Framework incluye consideraciones para abordar las cuestiones de privacidad y las libertades civiles durante su implementación. En ciertos sectores y organizaciones, estos problemas pueden ser directamente aplicables a la entrega fiable de servicios críticos; en otros sectores y organizaciones, estas cuestiones no pueden ser relevantes debido a la naturaleza de la información que las mismas organizaciones manejan.

6.2.3 Proceso de implementación del Framework y beneficios. El Framework y esta guía misma, están diseñados para ser lo suficientemente flexibles para ser usados tanto por las organizaciones del sector de las telecomunicaciones que cuenten con programas de Ciberseguridad totalmente maduros como por las que actualmente tienen programas menos desarrollados o que por el contrario no lo tienen del todo.

Cada organización podrá decidir cómo y dónde se utilizará el Framework basado en su propio entorno de trabajo (alcance). La elección de aplicar el Framework no implica que el enfoque actual de la gestión del riesgo de Ciberseguridad de dicha organización sea ineficaz o necesite ser reemplazado, más bien, significa que la organización desea aprovechar los beneficios que ofrece el Framework.

La aplicación del Framework proporciona un mecanismo para que las organizaciones:

- Describan su postura de Ciberseguridad actual en términos de funciones, Categorías y los resultados de las subcategorías.

- Describan el nivel actual en el que se encuentran respecto al Framework.

- Describan el objetivo actual y los Perfiles para sus programas de Ciberseguridad.

- Evalúen el progreso hacia los Perfiles de destino deseados.

- Identifiquen y prioricen las oportunidades de mejora en el contexto de un proceso continuo y repetible.

6.2.4 Realizar un mapeo ayuda a las organizaciones a: Identificar las brechas entre los resultados obtenidos en el enfoque que tiene la organización actualmente y los resultados definidos en el Núcleo del Framework.

La organización puede tomar medidas para hacer frente a estas brechas, o en última instancia, puede determinar que estas diferencias no son significativas para la gestión de sus riesgos de Ciberseguridad. Sin embargo, la organización puede beneficiarse de la identificación y documentación de estas diferencias para facilitar las comunicaciones sobre el uso del Framework dentro de la organización. Idealmente, el Framework se incorpora como parte de un programa de mejora de los procesos de gestión de riesgos de Ciberseguridad.

6.3 ESTANDARES Y NORMAS DE REFERENCIAS PARA EL DESARROLLO DEL FRAMEWORK

En esta sección se presenta una visión general de algunas normas de seguridad de la información y procesos existentes que actualmente son usadas por empresas del sector de las redes de telecomunicaciones, y que podrían llegar a apoyar el desarrollo de este Framework de Ciberseguridad.

- **Ejemplos de la gestión de riesgos de Ciberseguridad en el sector de las redes de telecomunicaciones.** Varias herramientas de gestión de riesgos de seguridad, procesos, normas y directrices ya ampliamente utilizados por las organizaciones del sector de las telecomunicaciones se pueden alinear bien con los enfoques de seguridad y de gestión de riesgos del Framework.

En relación con lo anterior, se revisará la correlación existente de algunas de estas normas actualmente utilizadas como son las ya familiares ISO27011, ISO27005 e ISO31000.

Un ejemplo de un conjunto de normas de gestión de riesgos de seguridad de la información utilizados en todo el sector de las telecomunicaciones se describe en la Cuadro a continuación:

Cuadro 1. Guías de referencia para el desarrollo del Framework

Nombre	Información	Referencia
ISO 27011	ISO 27011 aborda las directrices de gestión de seguridad para las organizaciones de telecomunicaciones basadas en la norma ISO 27002.	http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9332
ISO 27005	ISO 27005 es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información.	http://www.iso.org/iso/catalogue_detail?csnumber=56742
ISO 19000	El propósito de la norma ISO 31000:2009 es proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo.	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170

6.4 MAPEO DEL FRAMEWORK

Aunque la idea de realizar un mapeo del Framework puede llegar a parecer confusa, en realidad es muy sencilla. Básicamente las organizaciones pueden llegar a trazar, traducir o mapear su enfoque de Ciberseguridad actual para

llevarlos hasta los elementos que componen al Framework, usando estándares o normas específicas como guía cuando esto les sea posible. Realizar el mapeo no sólo soporta la habilidad de una organización para identificar las posibles deficiencias o brechas que necesiten ser tratadas, sino que también puede resaltar en qué lugar el Framework no está cumpliendo con su propósito (en caso de que este ya haya sido implementado) y en donde no describe adecuadamente el enfoque de Ciberseguridad de la organización. Básicamente y como conclusión, un mapeo claro puede llegar a proveer una traducción entre las prácticas actuales de la organización y el Framework de Ciberseguridad, soportando la comunicación al mismo tiempo con terceros o interesados externos.

6.5 ENFOQUE A LA IMPLEMENTACIÓN DEL FRAMEWORK

La sección a continuación presenta un enfoque estándar para un posible uso del Framework (Figura 40), que va de la mano con los siete pasos descritos en el Framework de Ciberseguridad desarrollado por NIST. Este enfoque puede ser utilizado junto con cualquier estándar de Ciberseguridad (en caso de alguna futura implementación oficial para Colombia), lineamientos o regulaciones específicos del sector (para este caso específico del sector de las telecomunicaciones), o una herramienta comercial para la gestión de los riesgos de Ciberseguridad.

Al realizar un análisis acerca de cómo debería llevarse a cabo la implementación del Framework de NIST en el sector de las telecomunicaciones, se deberían tener en cuenta las recomendaciones de la ITU (Unión internacional de Telecomunicaciones), así como la resolución 2258 de 2009 del CRC (comisión de regulación de comunicaciones), en donde se establecen las características generales que se deben cumplir para la seguridad de los datos e informaciones y la inviolabilidad de las comunicaciones. Para el caso de la gestión de riesgos de Ciberseguridad se podrá tomar como referencia las normas ISO 27005 e ISO31000.

Gráfica 14. Pasos del Framework de Ciberseguridad

Fuente: Ciberseguridad en Sistemas de Control Industrial en Infraestructuras críticas [en línea]. SCADALAB, 2014 [Consultado 8 de enero de 2015]. Disponible enInternet:http://www.infoplc.net/files/documentacion/ciberseguridad/infoPLC_net_SCADALAB_Modulo_2_Tema_2.pdf

Muchas organizaciones del sector de las telecomunicaciones en Colombia ya tienen programas integrales de gestión de riesgos de seguridad que establecen el contexto para la toma de decisiones basadas en el riesgo que les permite: evaluar el riesgo, identificación de la dirección que deben tomar los riesgos, y monitoreo de los riesgos de manera continua. Para estas organizaciones, las actividades descritas en estos siete pasos ya han sido probablemente llevadas a cabo, y la aplicación del Framework es en gran medida una cuestión de descripción, alineación o mapeo de los elementos de su enfoque actual a los elementos del Framework (Núcleo y Niveles).

6.5.1 Paso 1: Establecer prioridades y alcance. En este paso, la organización decide cómo y dónde se quiere usar el Framework (el alcance y el uso del mismo), ya sea en: uno o varios subconjuntos de sus operaciones (o procesos) o para toda la organización; lo que representaría una ventaja a la hora de establecer las prioridades en las áreas y objetivos sobre las cuales una organización plantea gestionar sus riesgos.

La decisión relacionada con dichos objetivos, es decir, *como* y *donde* debe aplicarse el Framework, debe basarse en consideraciones de la gestión del riesgo dentro de una organización y las políticas establecidas dentro de dichos programas. Algunas de ellas pueden estar ya establecidos dentro de una organización:

- Objetivos y prioridades organizacionales.
- Disponibilidad de recursos.
- Infraestructura critica.
- Factores de riesgo internos y externos.
- Información relacionada con vulnerabilidades y amenazas, actuales y específicas de Ciberseguridad sobre el sector de las telecomunicaciones.

La posible implementación del Framework puede llegar a ser compleja para organizaciones donde sus programas establecidos de gestión del riesgo no cuenten con el personal o la experiencia suficiente al momento de identificar o establecer prioridades relacionadas con los riesgos de Ciberseguridad.

Como consecuencia, podrían verse reflejadas dificultades cuando dichas áreas de gestión de riesgos deseen enfocar el Framework sobre toda la compañía al momento de intentar una implementación. Es posible entonces, que algunas de estas dificultades, puedan llegar a verse disminuidas si al momento de usar o aplicar el Framework, se hace sobre un pequeño subconjunto de las operaciones de un área en particular, para ganar familiaridad y experiencia sobre ella.

Una vez establecida dicha familiaridad, la organización puede llegar a considerar la aplicación del Framework sobre un conjunto de operaciones más amplio y de mayor envergadura; esto claro, depende en la forma en que la organización ha realizado con anterioridad la debida priorización y alcance de cada una de las áreas donde puede llegar a verse reflejado el riesgo.

A continuación se expondrá el resumen en una forma un poco más sencilla de esta primera etapa de prioridades y alcance. Se visualizarán las entradas y actividades para dicha fase, así como sus resultados:

Cuadro 2. Establecer Prioridades y alcance

Entradas	Actividades	Salidas
- *Estrategia de gestión del riesgo*. - *Información relacionada con bases de vulnerabilidades y amenazas*. - *Objetivos y prioridades organizacionales*.	- *La organización determina donde desea aplicar el Framework*. - *Definición del alcance.*	- *Uso del alcance que puede llegar a tener el Framework sobre el área en particular donde se ha aplicado, operación, o en la organización como tal.*

6.5.2 Paso 2: Orientar. Dentro de esta etapa la organización tomara los resultados obtenidos en el paso anterior e identificará los sistemas, los activos, los requerimientos, así como el enfoque en cuanto a Ciberseguridad y gestión de riesgos del área u operación donde se va a aplicar el Framework. Esto incluye las normas y prácticas que la organización ya utiliza, y que pueden incluir normas adicionales que puedan llegar a contribuir para el logro de sus objetivos de negocio y para la gestión de los riesgos de Ciberseguridad.

Para una identificación optima de los sistemas y activos mencionados con anterioridad, una de las recomendaciones propuestas por parte de NIST, es centrarse inicialmente en los sistemas y activos críticos, para luego ampliar el enfoque a los demás sistemas que representen menor criticidad para el desempeño de la empresa. Así mismo, la organización también debe determinar el enfoque de evaluación que utilizará para identificar su postura actual en cuanto a Ciberseguridad y gestión del riesgo. Las organizaciones pueden utilizar cualquiera de una serie de métodos de evaluación para identificar su postura de Ciberseguridad actual y crear un perfil actual (*dentro de los sistemas de gestión esta etapa seria el análisis de brecha* GAP).

Algunos de los aspectos claves mencionados para una organización al momento de una posible implementación:

- Describir su postura de Ciberseguridad.
- Describir su estado objetivo en materia de Ciberseguridad.
- Identificar y priorizar las oportunidades de mejora en el contexto de un proceso continuo y repetible.
- Evaluar el progreso hacia el estado objetivo o de destino.
- Comunicar entre las partes interesadas internas y externas, los temas relacionados con los riesgos de Ciberseguridad actual.

Basados en el Framework podemos resaltar que los perfiles pueden ser utilizados para identificar oportunidades de mejora en la postura de Ciberseguridad en una

organización, mediante la comparación del Perfil “actual” (*el estado "vigente" de dicha postura*) con un Perfil "objetivo" (*el estado deseado "a ser" de dicha postura*); el perfil actual puede ser utilizado para apoyar el establecimiento de prioridades y la medición del progreso hacia el Perfil de destino.

En resumen, en esta segunda etapa llamada *Orientar*, se analizará las entradas y actividades para dicha fase, así como sus resultados:

Cuadro 3. Paso 2: Orientar

Entradas	Actividades	Salidas
- *Uso del alcance del Framework*. - *Estrategia establecida de gestión del riesgo*.	- *La organización identifica los sistemas y los activos que están dentro del alcance del Framework (Por ejemplo: la gente, la información, la tecnología y las instalaciones).* - *Referencias informativas (por ejemplo: normas o estándares de Ciberseguridad y de gestión de riesgos, herramientas, métodos y directrices)*	- *Sistemas y activos identificados dentro del alcance. (Gestión de activos)* - *Requerimientos identificados dentro del alcance.* - *Estándares identificados de Ciberseguridad y de gestión de riesgos dentro del alcance*. - *Enfoques de evaluación para determinar posturas actuales de Ciberseguridad y de gestión del riesgo*.

6.5.3 Paso 3: Crear un perfil actual. Para el desarrollo de la fase 3, la organización crea un Perfil actual (*Current Profile*) e identifica su nivel de implementación actual (*Implementation Tier*) mediante el mapeo de las prácticas existentes de Ciberseguridad y de gestión de riesgos en la organización, con las descripciones específicas en el documento del Framework.

El propósito en la identificación y creación de un Perfil actual no es simplemente crear un mapa entre las prácticas organizacionales y los resultados de las categorías y subcategorías propuestas por NIST, sino también comprender el grado en que esas prácticas pueden llegar a alcanzar los resultados descritos en el Framework. Cabe resaltar, que para desarrollar un Perfil, una organización debe revisar todas las categorías y subcategorías propuestas por NIST, basándose en los objetivos de negocios y una evaluación de riesgos, determinando cuáles son los más importantes.

Para identificar el Perfil actual, la organización debe usar el enfoque de evaluación identificado en el paso dos, para el mapeo de su enfoque en materia de Ciberseguridad existente y sus resultados, junto con los resultados de las categorías y sub categorías establecidos. Las organizaciones pueden realizar estas valoraciones como parte de la evaluación del riesgo o tener procesos definidos que se pueden aprovechar para identificar su estado actual. Por ejemplo, muchas organizaciones internacionales realizan evaluaciones periódicas de sus programas de Ciberseguridad a través de auditorías internas y externas o actividades similares. Los resultados de estas actividades pueden describir cuales prácticas han sido llevadas a cabo para los sistemas y activos dentro del alcance, y que puedan ser utilizadas en esta tercera fase.

Es importante entender, que los Niveles de Implementación del Framework (*Tiers*) proporcionan un contexto de cómo una organización considera el riesgo en cuanto a la Ciberseguridad y los procesos para gestionar dicho riesgo.

Para este tercer paso de *Crear un perfil actual*, se analizarán las entradas y actividades para dicha fase, así como sus resultados:

Cuadro 4. Paso 3: Crear un perfil actual

Entradas	Actividades	Salidas
- *Enfoque de evaluación usado en el paso anterior para identificar su postura actual en cuanto a Ciberseguridad y gestión del riesgo*. - *Sistemas y activos identificados dentro del alcance*. - *Requerimientos identificados dentro del alcance*. - *Estándares identificados de Ciberseguridad y de gestión de riesgos dentro del alcance*.	- *La organización identifica su estado actual (Perfil) en materia de Ciberseguridad y de gestión de riesgo*.	- *Perfil actual (Current Profile)* - *Nivel de implementación actual (Implementation Tier)*

6.5.4 Paso 4: Llevar a cabo una evaluación de riesgos. Dentro de sus programas de gestión de riesgos, las organizaciones realizan de forma periódica evaluaciones de riesgos de Ciberseguridad que tienen como objeto identificar y evaluar los riesgos que están presentándose continuamente y determinar cuáles están fuera de los niveles de tolerancias actuales. Los resultados de dichas actividades ayudan a la organización en la creación y desarrollo del Perfil de destino o deseado, así como a la identificación de un nivel de implementación de destino u objetivo.

Para las organizaciones que cuentan con un programa de gestión de riesgos establecido actualmente, el realizar este tipo de actividad se convertirá en parte de la práctica habitual de negocios de la organización.

Para este cuarto paso de Llevar a cabo una evaluación de riesgos, se analizarán las entradas y actividades para dicha fase, así como sus resultados:

Cuadro 5. Paso 4: Llevar a cabo una evaluación de riesgos

Entradas	Actividades	Salidas
- *Uso del alcance del Framework*. - *Estrategia establecida de gestión del riesgo*. - *Estándares identificados de Ciberseguridad y de gestión de riesgos dentro del alcance*. - *Requerimientos identificados dentro del alcance*.	- *Desarrollar un análisis de riesgos para el área u operación de la organización que se encuentra dentro del alcance del Framework*. - Por cada evento potencial identificado en la evaluación de riesgos, determinar la probabilidad de que ocurra y el impacto en la organización.	- *Reportes de evaluación de riesgos*.

6.5.5 Paso 5. Creando un perfil de destino. Después de haber definido el Perfil actual en el paso 3, la organización define un Perfil de destino, también conocido como *Perfil deseado*. Para la creación de dicho *Perfil,* deben considerarse algunos factores además del Perfil actual; como se puede observar en la tabla resumen, algunos de estos factores son mencionados allí y tomados en cuenta como entradas para esta fase.

Según lo visto durante el paso 3, la organización crea un Perfil Actual y un nivel de implementación actual. Para este paso 5, además de determinar un Perfil de destino, la organización también determina un *Nivel de implementación de destino* o *deseado,* que se aplica dentro del alcance del proceso de gestión de riesgos.

El *Perfil de destino* identifica los resultados de la categoría y subcategoría deseados, así como los estándares de Ciberseguridad y de gestión de riesgos asociados (estándares, normas, herramientas, métodos y directrices que permitan mitigar los riesgos de Ciberseguridad de la organización).

Como se señaló en el paso 3, el Framework ofrece una amplia cobertura de los dominios de Ciberseguridad y de gestión de riesgos, mas sin embargo, no cubre todos los aspectos a abarcar. La organización puede llegar a ver la necesidad de implementar estándares, herramientas, métodos y directrices que permitan alcanzar los resultados que no estén definidos en el Framework, y los objetivos que estén alineados con las necesidades del negocio; uno de los aspectos a favor o ventajas que ofrece el Framework, es que el Perfil de destino también debe aportar a la identificación de estas prácticas mencionadas con anterioridad.

La organización entonces, examina cada nivel (*Tier*) y selecciona así mismo su nivel de implementación de destino (es decir, su nivel de implementación "*deseado*"). Una vez seleccionado dicho nivel, la organización identifica las prácticas de Ciberseguridad y las actividades de gestión de riesgos necesarias para lograr dicho objetivo o destino.

Con el uso de sus estándares de Ciberseguridad y de gestión de riesgos, herramientas, métodos y directrices, la organización documenta los resultados deseados en el Perfil de destino y en el Nivel de implementación deseado.

En este quinto paso de Crear un perfil de destino, se analizarán las entradas y actividades para dicha fase, así como sus resultados:

Cuadro 6. Paso 5: Creando un perfil de destino.

Entradas	Actividades	Salidas
- *Perfil y nivel de implementación actual.* - *Estrategia establecida de gestión del riesgo*. - *Objetivos organizacionales*. - *Practicas actuales de gestión de riesgos*. - *Entorno de riesgo actual.* - *Requerimientos legales y regulatorios*. - *Objetivos y misión de negocios.*	- *Determinar cuáles Categorías y subcategorías adicionales (como objetivos específicos de seguridad) deberían ser agregados al Perfil de destino para que cuente como parte del riesgo organizacional.*	- *Perfil de destino o deseado*. - *Nivel de implementación de destino o deseado*.

6.5.6 Paso 6: Determinar, analizar, y priorizar brechas. La organización evalúa su Perfil actual y el *Nivel de implementación actual* contra su *Perfil de destino* y su *Nivel de implementación de destino* e identifica las brechas (gaps). Existe una brecha cuando un resultado deseado de una categoría o subcategoría en el perfil de destino, o nivel de implementación de destino, no ha sido correctamente alcanzado por parte del enfoque existente de la gestión de riesgos de Ciberseguridad de la organización, así como cuando las prácticas actuales no logran el resultado con el grado de satisfacción exigida por la estrategia de gestión de riesgos de la organización.

Después de identificar las brechas tanto en el Perfil, como en el Nivel, la organización determina las posibles consecuencias de no abordar las brechas identificadas durante el proceso. Una prioridad de mitigación, debe ser asignada a todos las brechas identificadas. La priorización de las brechas debe incluir la consideración de las prácticas actuales en cuanto a gestión de riesgos, el entorno de riesgo actual, los requisitos legales y reglamentarios, los objetivos empresariales y de misión, y todas las restricciones organizacionales aplicables.

Una vez se le ha asignado la prioridad de mitigación a cada brecha, la organización identifica las respectivas y posibles actividades de mitigación, y lleva a cabo un análisis de costo-beneficio (*CBA*) en aquellas acciones potenciales. La organización debe entonces desarrollar un plan de acciones de mitigación priorizadas basado en los recursos disponibles, las necesidades del negocio, y el riesgo actual del entorno para pasar del estado actual al estado objetivo. Ahora, que si la organización se encuentra ya en su estado objetivo, sería importante para la organización tratar de mantener su postura de seguridad mientras el panorama de riesgos pueda llegar a cambiar.

Se debe tener en cuenta, que los resultados identificados y descritos en las Categorías y Subcategorías del Framework no pueden abordar todos los riesgos de Ciberseguridad de la organización. Sin embargo, el Perfil de destino debería incluir todos los posibles enfoques de Ciberseguridad (estándares, normas, herramientas y guías) que serán utilizados por la organización para hacer frente a los riesgos de Ciberseguridad.

En este sexto paso de Determinar, analizar y priorizar brechas, se analizará las entradas y actividades para dicha fase, así como sus resultados:

Cuadro 7. Paso 6: Determinar, analizar y priorizar brechas

Entradas	Actividades	Salidas
- *Perfil actual* - *Nivel de implementación actual (Tier)* - *Perfil objetivo* - *Nivel de implementación de destino* - *Estrategia de gestión del riesgo* - *Brechas y consecuencias potenciales* - *Impacto a la infraestructura critica*	- *Analizar las brechas entre el perfil actual y el deseado* - *Evaluar posibles consecuencias de las brechas identificadas* - *Determinar que brechas en particular necesitan atención y a cuales se les debe dar prioridad* - *Identificar acciones para abordar dichas brechas y priorizarlas* - *Realizar análisis costo-beneficios sobre dichas acciones a realizar*	- *Brechas identificadas, priorizadas y sus posibles consecuencias* - *Plan de acción y prioridades sobre dichas brechas identificadas*

6.5.7 Paso 7: implementar el plan de acción. Una vez se han determinado las *brechas* en el paso inmediatamente anterior, entre el Perfil actual y el de destino, la organización ejecuta el plan de implementación y realiza un seguimiento de su progreso a mediano o largo plazo (según la priorización con la que estas brechas han sido catalogadas), garantizando que las brechas se cierren y que los riesgos sean continuamente monitoreados.

Para este paso final de Implementar el *plan de acción*, analizaremos las entradas y actividades, así como sus resultados:

Cuadro 8. Paso 7: Implementar el plan de acción

Entradas	Actividades	Salidas
- *Plan de implementación priorizado.* - *Misión y objetivos organizacionales.*	- *Implementar acciones según prioridades previamente establecidas.* - *Seguimiento del progreso del plan de acción.* - *Monitoreo y evaluación continua del riesgo.*	- *Datos de seguimiento del proyecto, área u operación donde se ha realizado la implementación del Framework*. - *Implementación de nuevas medidas de seguridad, controles y monitoreo del riesgo*.

7. ADAPTACION DEL FRAMEWORK DE CIBERSEGURIDAD DE NIST AL MODELO COLOMBIANO

El éxito de NIST, sus modelos y estándares propuestos año tras año, y por lo tanto sus resultados hablan por sí mismos. Cierto es que hay trabajo por hacer y camino por recorrer para mejorar la gestión de riesgos y capacidades de Ciberseguridad independientemente del tamaño de las organizaciones que soporten infraestructuras críticas o no. Es debido a esto, que la identificación de brechas al momento de querer adaptar un estándar internacional a un ambiente Local es un factor fundamental en su propia capacidad de evolución; se espera dentro de esta investigación, a través de los puntos que se expondrán a lo largo de este capítulo, poder iluminar de alguna forma dichas brechas y en algún punto el camino para mitigarlas.

El Framework desarrollado por NIST fue pensado y desarrollado para reducir los riesgos de Ciberseguridad sobre infraestructuras críticas. Sus funciones, etapas y procesos, como se vio en este documento dan una impresión bastante sólida y positiva ya que el cubrimiento que realizan es bastante extenso y da un entendimiento más amplio en cuanto a lo que representa implementar la seguridad. Sin embargo, en el proceso de investigación realizado en este documento, al recorrer el Framework se encontraron algunas brechas perceptibles al momento de querer realizar una posible implementación a un modelo como el colombiano. Brechas como la ausencia de entidades gubernamentales o privadas enfocadas en la seguridad sobre las infraestructuras críticas, así como personal debidamente capacitado y certificado en la administración y gestión de infraestructuras críticas, serán tratadas en este capítulo.

La conciencia de la necesidad de mejorar es a menudo el catalizador para el cambio, y la evidencia proporcionada durante este trabajo de investigación, podría llegar a constituir un poderoso incentivo para la mayoría de las organizaciones que soportan infraestructuras críticas para desarrollar un plan enfocado de mejora.

Ausencia de entidades públicas y privadas especializadas en el área de Seguridad en infraestructuras críticas. Al momento de comenzar a evaluar la posible adaptación del Framework de Ciberseguridad de NIST al medio colombiano se empezaron a identificar brechas de seguridad que evidencian una gran diferencia en el nivel de madurez entre países como Colombia y Estados Unidos, esto

debido a que Estados Unidos se encuentra a la vanguardia en cuanto a temas de Legislación, Tecnología y Ciberseguridad, entre otros.

Como primera brecha se encontró que en las funciones de responder y recuperar se encuentra una categoría denominada Comunicaciones, la cual hace referencia a las entidades internas y externas (siendo esta ultima la más relevante en este proyecto de investigación) que tienen como función recibir información sobre cambios, incidentes o mejoras en sus planes de Ciberseguridad. Dicha retroalimentación permite que los sectores y el medio se mantengan constantemente informados sobre los nuevos ataques o mejoras en planes de Ciberseguridad, aportando a la consolidación de buenas prácticas y promoviendo constante investigación en temas referentes a la Ciberseguridad y la protección de infraestructuras críticas.

Queda claro que para el Framework de Ciberseguridad de NIST la categoría de Comunicación es muy importante, ya que gran parte del entendimiento de las acciones realizadas en el momento de emprender un plan de respuesta y de recuperación viene de experiencias sucedidas en el medio. Debido a esto, es importante que existan asociaciones gubernamentales y privadas que colaboren compartiendo este tipo de información. En Colombia actualmente las entidades que están al tanto de los temas de Ciberseguridad y respuesta a incidentes son el Colcert y el CSIRT, dichas entidades son globales y no le apuntan a ningún sector de las infraestructuras críticas en específico, y que por lo tanto no abarcarían en su totalidad todos los requerimientos de cada uno de los sectores, lo que conllevaría a que el canal de comunicación para compartir información que propone el Framework de NIST no sea eficiente.

Como parte de la investigación de este trabajo de grado se propone la siguiente estructura jerárquica en la cual se muestra cada uno de los entes que intervendrán en la protección de infraestructuras críticas a nivel nacional.

Gráfica 15. Modelo propuesto

:

En el ámbito de la protección de infraestructura críticas a nivel nacional se deberán encontrar involucrados un conjunto de organismos y entidades, pertenecientes tanto al sector público como al sector privado los cuales en conjunto ayudaran a la protección de las infraestructuras en cada uno de los sectores críticos del país.

El ministerio de Defensa en conjunto con el Ministerio de las Tecnologías de la Información deberán ser los órganos superiores responsables del Sistema de Protección de Infraestructuras críticas, estos serán los encargados de la creación de leyes y lineamientos de políticas para la Ciberseguridad y Ciberdefensa nacional de dichas infraestructuras. Además será indispensable la creación de entidades que respalden a estos órganos superiores. Las entidades propuestas serian el Centro Colombiano para la Protección de las Infraestructuras Críticas y la Comisión Estratégica Colombiana para la Protección de Infraestructuras Críticas. El primero deberá ser el órgano responsable de la supervisión, coordinación e impulso de las actividades vinculadas a la protección de

infraestructuras críticas. El segundo será el encargado de aprobar los planes estratégicos sectoriales y la designación de operadores críticos.

El CSIRT y el COLCERT serán los encargado de la coordinación de atención a incidentes de Ciberseguridad y Seguridad informática a nivel nacional, deberán estar en contacto directo con los centros de seguridad de las empresas que manejen infraestructuras críticas y estar en capacidad de coordinar el tratamiento, solución de las solicitudes y denuncias sobre problemas de Ciberseguridad. De igual forma, también deberán mantener una comunicación constante con organizaciones internacionales que trabajan en el sector de la Ciberseguridad y hacer uso de información especializada entregada por estas, de esta forma advertir a los sectores afectados sobre cualquier tipo de contenido o actividad maliciosa que pueda tener alojadas dentro de sus redes, y que afecte directamente su operación, o amenace la seguridad de sus clientes.

En el siguiente nivel de la estructura jerárquica estarán las organizaciones de Ciberseguridad por cada uno de los sectores críticos y serán las encargadas de reunir toda la información relacionada con las brechas de seguridad encontradas en sus respectivas infraestructuras, así como las tendencias de los ataques en cada uno de los sectores. Esto servirá como punto de partida para iniciar una comunicación proactiva entre cada uno de los proveedores del mismo sector y tener una base de datos solida e histórica de los principales acontecimientos.

En el último nivel de la estructura, estarán los operadores críticos. Estos juegan un papel determinante dado que son los responsables de elaborar los planes de seguridad del operador así como los planes de protección específicos para cada una de las infraestructuras que se encuentre bajo su responsabilidad.

Ausencia de personal debidamente capacitado. Una vez establecidas dentro del modelo colombiano dichas entidades que de forma pública o privada velarán por la seguridad de las infraestructuras críticas, podría concluirse entonces que las mismas, deberían contar con el personal idóneo para desempeñarse en la labor que estas llegarán a representar. Sin embargo, como se describió en la brecha identificada con anterioridad, al no contar con dichas entidades dentro de una estructura ya establecida y robusta, los esfuerzos por tener personal altamente capacitado serían mayores, divididos y recaerían principalmente sobre otros sectores como el académico.

La presencia de personal idóneo que capacitado y certificado para administrar y gestionar infraestructuras críticas, permitirá obtener los conocimientos necesarios, así como una serie de competencias y experiencias en el campo técnico que necesita Colombia para alcanzar los objetivos deseados en cuanto a Ciberseguridad.

Para establecer los lineamientos en cuanto a Ciberseguridad, es de carácter primordial contar con personal altamente calificado en los diferentes niveles: entes privados o de gobierno, operativo, técnico y judicial. De igual forma promover e impulsar las habilidades técnicas y de gestión para disponer de soluciones confiables que permitan proteger de forma idónea las infraestructuras criticas nacionales frente a posibles amenazas. Para lograr este grado de confiabilidad, se necesita fomentar y promover actividades de mejora continua en cuanto a lo concerniente a Ciberseguridad. Para esto será primordial la colaboración entre oficiales de seguridad que hagan parte de los sectores que soportan infraestructuras críticas, favoreciendo la colaboración entre organizaciones del sector público y privado fomentando así la investigación, capacitación y posterior certificación de la Ciberseguridad. La capacitación adecuada del personal a cargo de la gestión e implementación de la Ciberseguridad se convertiría en un objetivo primordial para las organizaciones. Promover la capacitación de profesionales y reforzar los planes de acción en cuanto a respuesta y recuperación en materia de Ciberseguridad.

Las iniciativas descritas a continuación, serán necesarias para obtener el conocimiento y las competencias en un nivel adecuado por parte de los profesionales en materia de Ciberseguridad.

- Desarrollar un Marco establecido que abarque y contemple conocimientos de Ciberseguridad en los campos operativo, técnico y regulatorio.

- Invertir en los programas de investigación y certificación en Ciberseguridad enfocados a las infraestructuras críticas en cooperación con Universidades e institutos internacionales.

- Constituir mecanismos que permitan de forma temprana identificar las demandas y prioridades en materia de Ciberseguridad como parte de un organismo cambiante.

- Promover el desarrollo de servicios y materiales relacionados con la Ciberseguridad para impulsar la competitividad, la divulgación internacional,

oportunidades de mejora, la eliminación de barreras, orientación y alineación normativa, entre otras.

- Promover la creación de planes Nacionales de Investigación, concursos de Innovación Técnica, así como iniciativas que fomenten a su puesta en práctica e internacionalización.
- Impulsar la coordinación y comunicación entre los organismos y organizaciones que trabajando en conjunto persiguen un mismo objetivo y estado de Ciberseguridad.

- Impulsar a la participación en convocatorias y concursos como parte del proceso de certificación de Ciberseguridad de acuerdo con los estándares y normas internacionales.

- Formalizar los procesos y criterios en cuanto a adquisición de sistemas, productos y su respectivo desarrollo.

- Promover la creación y desarrollo de modelos y técnicas de análisis e identificación de Ciberamenazas, protección de sistemas específicos de infraestructuras críticas, así como su respectiva evaluación y certificación.

Adicional a las iniciativas mencionadas con anterioridad, se propone ofrecer las siguientes capacitaciones o certificaciones específicas por parte del gobierno colombiano a través del MinTIC y el Ministerio de defensa Nacional, a las cuales se podría acceder a través de becas y concursos. De esta forma, los profesionales en seguridad de la información puedan estar a la vanguardia en cuanto a estándares internacionales, así como a la tendencia en cuanto a amenazas vivas y cambiantes, al momento de enfrentarse en forma real a los retos que supone el manejo de la seguridad sobre infraestructuras críticas. Estas capacitaciones y certificaciones que se proponen para cubrir dichos aspectos, se reúnen a continuación:

- Certificados ISA. La norma ISA99 y su evolución IEC 622443 son dos normas que enfocan sus esfuerzos en la seguridad de los sistemas de control sobre organizaciones que soporten grandes infraestructuras. Dicha norma engloba un conjunto de guías e informes técnicos que describen los elementos necesarios para la implantación de un sistema de gestión de la Ciberseguridad y cómo conocer los requerimientos de cada elemento, herramientas de seguridad, al igual que su modo de implantación y despliegue dentro de los sistemas de control.

La ISA entonces ha definido cinco certificados que se complementan entre sí, y las cuales pueden contribuir a que los profesionales que gestionan la seguridad sobre infraestructuras críticas incrementen sus conocimientos sobre sistemas de control:

- Certificate 1: ISA99/IEC 62443 Cybersecurity Fundamentals Specialist
- Certificate 2: ISA99/IEC 62443 Cybersecurity Risk Assessment Specialist
- Certificate 3: ISA99/IEC 62443 Cybersecurity Design Specialist
- Certificate 4: ISA99/IEC 62443 Cybersecurity Maintenance Specialist
- ISA99 Cybersecurity Expert

Los certificados mencionados con anterioridad están orientados hacia profesionales que trabajen en entornos TI relacionados con la seguridad, y que vean la necesidad de mejorar su conocimiento en cuanto a temas de Ciberseguridad; con anterioridad se mencionaba que dichos certificados se complementaban entre sí, esto debido a que los mismos deben ser realizados en un orden en específico y permiten al candidato mejorar el conocimiento obtenido en el anterior. Al ser un certificado y no una certificación no requiere de renovación.[2]

- Global Industrial Cyber Security Professional (GICSP). La certificación GICSP une al entorno TI, ingeniería y Ciberseguridad para mejorar la seguridad en los sistemas de control industrial, desde el diseño hasta su retirada. Es independiente del sector industrial relacionado, y se centra en garantizar un conjunto mínimo de conocimientos y capacidades que los profesionales de TI, ingenieros y especialistas en seguridad deben conocer si su trabajo está relacionado de algún modo con la seguridad de los sistemas de control industrial.

  Dicha certificación es auspiciada por la Global Information Assurance Certification (GIAC), empresa dedicada a las certificaciones de seguridad. El GICSP se creó en un esfuerzo colaborativo entre diferentes industrias relacionadas con el diseño, despliegue, operación y/o mantenimiento de sistemas e infraestructuras de automatización y carácter crítico. Esta

[2] ISA.ORG. ISA/IEC 62443 Cybersecurity Certificate Programs [En línea]. Disponible en: https://www.isa.org/isa-certification/certificate-programs/ [Consultado 18 Enero 2016].

certificación puntualmente por ejemplo, consiste en un único examen, y debe ser renovada cada 4 años.[3]

- Certified SCADA Security Architect (CSSA). Esta certificación verifica mediante un examen, los conocimientos que un profesional posee en seguridad de sistemas de control industrial, y está orientada principalmente hacia los sectores energéticos, como distribución eléctrica, gas/petróleo y el tratamiento de aguas.

  La certificación beneficia tanto a los profesionales del sector al confirmar sus conocimientos teóricos y su compromiso en seguridad, como a las empresas a las que asegura los conocimientos necesarios de sus trabajadores, y verifica la preparación en puestos con un alto nivel técnico. Aparte, también permite crear una red de expertos en Ciberseguridad y proporciona un valor diferencial ante la competencia.
  La certificación CSSA está pensada para administradores de redes industriales y profesionales del sector TI así como sus respectivos responsables. La misma, surge de la mano de la Information Assurance Certification Review Board (IACRB), entidad global centrada en la certificación de profesionales en seguridad.[4]

- ISA Certified Automation Professional (CAP) Certification Program. Como uno de los certificados más valorados ISA CAP ofrece una valoración de las habilidades de un profesional sobre la automatización de forma objetiva, imparcial e independiente. La certificación se obtiene a través de un examen centrado en:

  - Dirección, definición, diseño, desarrollo/aplicación, implementación, documentación y soporte de los sistemas.

  - Software y equipos utilizados en los sistemas de control.

  - Sistemas de información de fabricación.

[3] GIAC.ORG. Global Industrial Cyber Security Professional (GICSP). [En línea]. Disponible en: http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp [Consultado 16 Enero 2016].
[4] IACERTIFICATION.ORG. Certified SCADA Security Architect (CSSA). [En línea]. Disponible en: http://www.iacertification.org/cssa_certified_scada_security_architect.html[Consultado 18 Enero 2016].

- Integración de sistemas.
- Consultoría operacional.

Los profesionales certificados con ISA CAP son un grupo de expertos que han demostrado poseer un amplio conocimiento de la automatización y el control. La certificación evidencia que poseen experiencia y cualificación suficiente para desempeñar su trabajo.[5]

- ISA Certified Control Systems Technician (CCST). Esta certificación ofrece tres niveles diferentes dependiendo de la experiencia, educación y formación recibida, siendo el nivel III el más elevado. El examen de certificación de CCST cubre cuatro aspectos principales de las tareas relacionadas con los técnicos de los sistemas de control. Los temas se han elegido de forma internacional después de un estudio llevado a cabo sobre el sector. Destinada a técnicos y operadores de los sistemas de control, principalmente de áreas neumáticas, electrónicas, mecánicas y de instrumentación. Muchas grandes empresas a nivel global apoyan la certificación CCST de la ISA.[6]

En conclusión las certificaciones de seguridad suponen una parte primordial en los entornos de seguridad relacionados con las tecnologías de la información, y son un requisito habitual (obligatorio en algunos casos) para la ejecución de cualquier proyecto. Dichas certificaciones cubren temas y áreas especializadas como pruebas de penetración, análisis forense, seguridad en sistemas SCADA, Ciberseguridad, auditoría de sistemas, etc. Y terminan convirtiéndose en piezas claves para organizaciones al momento de querer confirmar los conocimientos de sus oficiales de seguridad.

Al ofrecer las oportunidades de acceder a dichas capacitaciones y certificaciones, los entes mencionados con anterioridad, contribuirían a asegurar el conocimiento de profesionales que finalmente retribuirían dicho conocimiento en acciones reactivas y proactivas, cuyo objetivo final no solo recaería en la seguridad general de TI, sino también sobre la robustez en materia de Ciberseguridad y la protección de las organizaciones que soportan infraestructuras críticas. Por esta razón, los

[5] ISA.ORG. ISA Certified Automation Professional (CAP) Certification [En línea]. Disponible en: https://www.isa.org/templates/two-column.aspx?pageid=53023 [Consultado 18 Enero 2016].
[6] ISA.ORG. ISA Certified Control Systems Technician (CCST) [En línea]. Disponible en: https://www.isa.org/templates/two-column.aspx?pageid=53024 [Consultado 18 Enero 2016].

conocimientos y la experiencia del personal que pretenda concursar y opte ser candidato a dichas certificaciones, son claves en la obtención de la misma. Las certificaciones en materia de seguridad generalmente consisten en un único examen, y deben ser renovadas cada 3 o 4 año.

8. CONCLUSIONES

Es imperativo que las empresas u organizaciones que soportan infraestructuras críticas del país, como lo son las que pertenecen al sector de las telecomunicaciones, tengan establecido dentro de sus procesos los modelos o estándares de Ciberseguridad que permitan de alguna forma la gestión de los riesgos inherentes a dichas infraestructuras y los servicios que soportan. Es importante mencionar, que aunque un tema como la Ciberseguridad es conocido en las organizaciones y lo es en cierta forma familiar, tal vez no se le da en la actualidad la relevancia que merece. Debe tenerse en cuenta y entenderse, que no solo el conocimiento y los avances en el dominio de este tema pueden llegar a permitir que las organizaciones enfrenten los riesgos relacionados a la Ciberseguridad; el uso de estándares probados y aceptados internacionalmente les permitirá alcanzar no solo los niveles de Ciberseguridad deseados, sino también los objetivos de negocio específicos para cada empresa.

El Framework de Ciberseguridad desarrollado por NIST permite cierta autonomía en las organizaciones que deciden tomar dicho estándar dentro de sus programas de gestión del riesgo. Para Colombia, y sus organizaciones de infraestructuras críticas, el Framework podría adaptarse casi en su totalidad a las necesidades del país, a excepción de algunas brechas las cuales fueron identificadas en el capítulo anterior; lo que permite concluir que aunque dicho Framework es pensado, desarrollado y aplicado internacionalmente, no es exclusivo. Una de las ventajas más importantes y que más llamaron la atención del Framework desarrollado por NIST, es el hecho de ofrecer la posibilidad de dar un punto de partida para la creación de áreas encargadas de la gestión de los riesgos de Ciberseguridad, en caso de que las organizaciones no cuenten con una.

Parte de los objetivos que se plantearon para este proyecto consistían en realizar una guía que motivara y llevara a las organizaciones a visualizar una posible y futura implementación del Framework de Ciberseguridad desarrollado por NIST. Al validar un modelo o estándar desarrollado e implementado con éxito, que además cuenta con las características de ser adaptativo y flexible, en países con infraestructuras críticas, se observa que dichas iniciativas pueden llegar a proveer resultados positivos además de acortar y allanar el camino en cuanto a materia de Ciberseguridad.

En sí misma, la guía elaborada en este documento muestra una visión general de ciertos aspectos, como conceptos y definiciones que componen al Framework, y otros un poco más profundos, donde se plantea la estrategia, posición actual en materia de Ciberseguridad y los pasos a seguir, si una organización se plantea la posibilidad de abordar con seriedad dicho tema de acuerdo a las normatividades del país donde se desee implementar (por ejemplo Colombia) y así mismo a las necesidades únicas que hacen parte de sus infraestructuras críticas.

Al analizar a las organizaciones en Latinoamérica, así como su postura y entendimiento de la Ciberseguridad como se vio en el estudio realizado por la OEA, puede verse que una de las mayores debilidades de las organizaciones se encuentra en su capacidad de medir, evaluar y mitigar los riesgos de Ciberseguridad, lo que hace que en algún punto sea difícil o imposible dar prioridad a las actividades de seguridad y la inversión que esta representa. Todavía las organizaciones dan demasiado énfasis en la etapa protección aun sobre las de detección y la respuesta, a pesar del hecho de que las capacidades de protección preventiva por si solas son en gran medida incapaces de detener las amenazas más grandes de Ciberseguridad hoy en día. La capacidad de detectar y responder a los ataques cibernéticos antes de que ocasionen daños o pérdidas, es una de las características más importantes que las organizaciones deben desarrollar y perfeccionar.

En el proceso de investigación realizado en este documento, al recorrer el Framework se encontraron algunas brechas perceptibles al momento de querer realizar una posible implementación a un modelo como el colombiano. Brechas como la ausencia de entidades gubernamentales o privadas enfocadas en la seguridad sobre las infraestructuras críticas, así como personal debidamente capacitado y certificado en la administración y gestión de dichas infraestructuras.

Finalmente se puede concluir, que si es posible realizar una adaptación del Framework al modelo colombiano teniendo en cuenta las brechas identificadas y las recomendaciones realizadas en este documento. Los puntos propuestos en este trabajo de investigación, darían una visión general respecto al estándar propuesto por NIST, así como temas referentes a Ciberseguridad, facilitando a las organizaciones pensar en la posible adaptación e implementación de este estándar a sus procesos que soporten infraestructuras críticas.

9. RECOMENDACIONES

Para una posible y futura implementación del Framework de Ciberseguridad de NIST, las organizaciones deberán entender y definir de forma objetiva sus posturas en cuanto a Ciberseguridad, en caso dado claro está, que las organizaciones cuenten en la actualidad con dicho programa.

Las organizaciones deberán entender el valor que tiene para sus procesos y objetivos de negocio la necesidad de contar con programas de Ciberseguridad basados en estándares internacionales, estos no solo pretenderán reforzar y mejorar dichos programas, sino también ayudar a aquellas organizaciones que no cuentan con ellos a que encuentren las bases para construir uno.

La presente investigación busca aportar y recomendar de igual forma, que en el caso dado que las organizaciones que soportan infraestructuras críticas, no vean la necesidad inmediata de implementar un estándar de Ciberseguridad, si puedan llegar a planteárselo dentro de un futuro plan de desarrollo. Dichas organizaciones, deberán comprender, que el Framework desarrollado por NIST puede llegar a ser aplicado e implementado en todos los procesos de la organización, así como solo en aquellos que se consideren de carácter crítico.

Consecuente con la idea anteriormente plateada, para una posible implementación de un estándar de seguridad dentro de una organización con políticas y procesos ya definidos, se requiere un poco más que una simple revisión del Framework. Es fundamental que las organizaciones cuenten con el personal idóneo en el momento de embarcarse en futuras implementaciones. De la capacidad de los profesionales encargados de la seguridad de las infraestructuras críticas, y su adecuada preparación, así como de su acertada comprensión de lo que busca cualquier estándar de Ciberseguridad, depende que los procesos y sistemas que soportan dichas infraestructuras mantengan su funcionamiento adecuado y constante.

No sobra mencionar y recomendar entonces, que las organizaciones pertenecientes al sector objeto de estudio, y el factor humano que hace parte de ella, entiendan de forma absoluta cómo funcionan las infraestructuras que operan y soportan, y el por qué mismo de su factor crítico. La necesidad de entender los

elementos que componen dichas infraestructuras críticas, y los requerimientos para soportar las mismas, debe ser inherente a los servicios que pretenden prestar, así como las responsabilidades que conllevan. El presente trabajo de investigación, propone una estructura jerárquica en la cual se muestra cada uno de los entes que intervendrían en la gestión de la protección de infraestructuras críticas a nivel nacional.

BIBLIOGRAFÍA

BEJARANO, María José. Estrategia de ciberseguridad nacional. 9 de diciembre del 2013. [En línea], [consultado el 2 de abril de 2015]. Disponible en: http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf

ISACA. Implementing the NIST Cybersecurity Framework. 2014. [En línea], [consultado el 2 de abril de 2015]. Disponible en: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/implementing-the-nist-cybersecurity-framework.aspx

MINISTERIO DE TECNOLOGÍA DE LA INFORMACIÓN. Lineamientos de política para ciberseguridad y Ciberdefensa. [En línea], [consultado el 2 de abril de 2015]. Disponible en: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

INSTITUTO ESPAÑOL DE ESTUDOS ESTRATEGICOS. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. . [En línea], [Consultado el 8 de abril de 2015]. Disponible en: https://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Framework for Improving Critical Infrastructure Cybersecurity. Febrero 12, 2014. [En línea], [consultado el 2 de abril de 2015]. Disponible en: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

UNIÓN INTERNACIONAL DE LAS TELECOMUNICACIONES. Guía de Ciberseguridad para países en desarrollo. 2007. [En línea], [consultado el 2 de abril de 2015]. Disponible en: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf